مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية

The Degree of Effectiveness of Internal Control Procedures in Providing Electronic Information Security in Jordanian Manufacturing Companies

إعداد الطالب

يوسف خليل يوسف عبدالجابر

401020023

إشراف

الدكتور مضر عبداللطيف

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في المحاسبة

قسم المحاسبة والتمويل– كلية الأعمال

جامعة الشرق الأوسط

كانون الثاني – 2013

تفويض

أنا الطالب يوسف خليل يوسف عبدالجابر أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي ورقيا والكترونيا للمكتبات، أو المنظمات، أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: يوسف خليل يوسف عبدالجابر

التاريخ: 13-1-2013

التوقيع:

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها" مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية " وأجيزت بتاريخ 13-1-2013

أعضاء لجنة المناقشة:

الاسم	الجامعة	التوقيع
1) د. مضر علي عبداللطيف / مشرفا ورئيساً	- جامعة الشرق الأوسط	
2) د. خالد جمال جعارات / عضوا داخلياً	- جامعة الشرق الأوسط	
3) د. بشير أحمد خميس / ممتحنا خارجياً	- الجامعة الأردنية	

الشكر والتقدير

قال تعالى { فَتَعَالَى اللَّهُ الْمَلِكُ الْحَقُّ وَلَا تَعْجَلْ بِالْقُرْآنِ مِنْ قَبْلِ أَنْ يُقْضَى إِلَيْكَ وَحْيُهُ وَقُلْ رَبِّ زِدْنِي عِلْمًا} [طه : 114]

بداية أحمد الله وأشكره شكراً كثيراً طيباً مباركاً، يا رب لك الحمد كما ينبغي لجلال وجهك وعظيم سلطانك على فضلك وتوفيقك لي لإنجاز هذا العمل.

الشكر والثناء إلى أستاذي الدكتور مضر عبد اللطيف الذي قبل الإشراف على رسالتي فكان قبولا حسنا، وأشرف فكان إشرافا أميناً، وعلّم فكان تَعليما متقناً، وجزاه الله خير الجزاء.

والشكر إلى أساتذتي في جامعة الشرق الاوسط لما قدموه لي من علم ومعرفة ومنهم الأستاذ الدكتور عبد الناصر نور والأستاذ الدكتور محمد مطر والأستاذ الدكتور محمد النعيمي والدكتور أسامة جعارة والدكتور عدنان الأعرج والدكتور محمد الشورة والشكر إلى لجنة المناقشة التي تفضلت بقبول مناقشة الرسالة.

الشكر والثناء إلى من كللهما الله بالهيبة والوقار... إلى من علماني العطاء بدون انتظار .. إلى والدي العزيزين كل الشكر والتقدير.

والشكر والثناء إلى رفيقة دربي وأم أولادي ... إلى زوجتي الحبيبة تمارا.

والشكر موصول إلى زملائي وزميلاتي في جامعة الشرق الأوسط الذين قدموا لي كل مساعدة طلبت منهم من نصح وإرشاد وتوجيه وأخص بالذكر الزملاء زيد الشوابكة وعامر العرموطي ولكل من مد لي يد العون والمساعدة.

الإهداء

إلى والديّ العزيزين

إلى زوجتي الحبيبة

إلى ولديّ الحبيبين تالا وخليل

إلى كل من كان سببا في وصولي إلى ما وصلت إليه

فهرس المحتويات

فهرس الجداول

الملخص باللغة العربية

مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية

إعداد يوسف خليل عبد الجابر

إشراف الدكتور مضر عبد اللطيف

هدفت الدراسة إلى السعي لاكتشاف مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية المستخدِمة لنظم المعلومات المحاسبية الإلكترونية في تخفيض مخاطر أمن المعلومات لديها والمعوقات التي تؤثر على فاعلية هذه الإجراءات من خلال تحديد ثلاثة مخاطر تهدد أمن نظم المعلومات وهي مخاطر اختراق الشبكات ومخاطر الهندسة الاجتماعية وأخيراً مخاطر البرمجيات الضارة، كما غطت فاعلية الرقابة الداخلية في منع واكتشاف المخاطر وتصحيحها في حالة وقوعها.

ولتحقيق هذا الغرض تم تصميم استبانة وقد تم توزيعها على عينة الدراسة المكونة من ثلاثين شركة صناعية عاملة في المملكة الأردنية الهاشمية تستخدم نظم المعلومات المحاسبية. ولتحليل البيانات قام الباحث باستخدام أساليب إحصائية تمثلت في المتوسطات الحسابية والانحرافات المعيارية واختبار كروسكال والس واختبار مان وتني واختبار One Sample t-test.

أظهرت نتائج التحليل الإحصائي فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية من خلال أوجهها الثلاثة (المنع والاكتشاف والتصحيح)

من خلال اختبار ثلاثة أنواع من المخاطر التي تهدد أمن المعلومات الالكترونية وهي مخاطر اختراق الشبكات والهندسة الاجتماعية والبرمجيات الضارة، كما أظهرت النتائج فروق ذات دلالة إحصائية بين إجابات أفراد العينة تعود للخلفية الشخصية لكل منهم خاصة في مجالات طبيعة الدور الوظيفي وسنوات الخبرة وحيازة شهادات مهنية وحجم الشركة وكونها أجنبية أو محلية.

أظهرت النتائج أيضاً وجود معوقات وتحديات تواجه تطبيق إجراءات رقابة داخلية فعالة ومنها عدم مواكبة التطور المتسارع لأساليب الاحتيال الإلكتروني، وأيضا عدم دعم الإدارة لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات.

لقد اقترحت الدراسة مجموعة من التوصيات منها ضرورة دعم الإدارة لأنشطة الرقابة الداخلية على أمن المعلومات من خلال توفير الكوادر المؤهلة، وكذلك تحفيز العاملين في الشركات الصناعية للحصول على الشهادات المهنية ذات العلاقة.

ABSTRACT

The Degree of Effectiveness of Internal Control Procedures in Providing Electronic Information Security in Jordanian Manufacturing Companies

Prepared by:

Yousef Khalil Abdel Jaber

Supervised by:

Dr. Modar Abdullatif

This study aimed to explore the degree of effectiveness of internal control procedures in Jordanian manufacturing companies that use electronic accounting information systems in reducing information security risks. In addition, the study covered the possible obstacles that limit the effectiveness of internal control in these companies. The study identified three general groups of risks (hacking, social engineering, and malware), and covered the effectiveness of internal controls in preventing and detecting these risks, and correcting the situation in case of their occurrence.

To achieve its aims, the study employed a questionnaire that was administered to thirty manufacturing companies operating in Jordan that use electronic accounting information systems. To analyze the findings, the researcher used statistical methods including means, standard deviations, Kruskal-Wallis and Mann –Whitney tests, and one-sample t-tests.

The findings showed that internal control procedures used by the companies are generally effective in preventing and detecting risks related to hacking, social engineering and malware, and in correcting their effects in case of their occurrence. In addition, the findings showed statistically significant differences in views of the study sample that may be attributed to the respondent's job nature, professional experience, and possession of a

professional certificate, and to the company's size and affiliation with an international company.

The results also showed the presence of obstacles and challenges facing the application of effective internal control procedures, including the rapid development of electronic fraud methods and the lack of management support for the activities of internal controls related to information security.

The study suggested a number of recommendations including management support for the activities of internal control over information security through the provision of qualified personnel, and encouraging them to obtain related professional certificates.

الفصل الأول

مقدمة عامة للدراسة

الفصل الأول

مقدمة عامة للدراسة

1-1 تمهيد

2-1 مشكلة الدراسة وأسئلتها

3-1 فرضيات الدراسة

4-1 هدف الدراسة

5-1 أهمية الدراسة

6-1 حدود الدراسة

7-1 التعريفات الإجرائية

1-1 تمهيد:

واجهت منظمات الأعمال العديد من التحديات المرتبطة بازدياد المنافسة في جميع المجالات والتي كان من أهم أسباب ظهور هذه التحديات ما يسمى بالعولمة والتطور التكنولوجي اللذين ساهما بدورهما في إزالة الحواجز والحدود بين منظمات الأعمال من جهة والعملاء من جهة أخرى، إذ أصبحت الحدود بين الدول أخر ما يعيق المنظمة في تحقيق أهدافها في الانتشار حول العالم.

وقد ظهرت أنظمة المعلومات المحاسبية الإلكترونية (Electronic Accounting Information Systems - EAIS) كأحد نتائج هذا التطور التكنولوجي المتسارع، حيث انتشرت هذه الأنظمة بسرعة كبيرة مدفوعة بعدة عوامل منها الحاجة لتوفير المعلومات الملائمة والموثوقة والتي تساعد الإدارة على اتخاذ القرارات المناسبة، من حيث استخدام الموارد المحدودة بالشكل الأمثل لمواجهة المنافسة المتزايدة على الصعيدين المحلي والدولي، وأيضا ازدادت حاجة المنظمات لهذه النظم بسبب انتشار فروعها سواء حول العالم أو داخل البلد الواحد، بالإضافة لتطور العمليات وتعقيدها وصعوبة تعامل العنصر البشري مع هذا الحجم الهائل من البيانات الناتجة عنها.

بالإضافة لذلك نتج عن ظهور أنظمة المعلومات المحاسبية الإلكترونية العديد من التحديات والمخاطر التي لم تكن معروفة في السابق والتي تستدعي من إدارة الشركة أن تقوم بتطوير أنشطة الرقابة الداخلية لديها من خلال إعداد السياسات والإجراءات التي تتيح الرقابة على هذه الأنظمة الإلكترونية.

ومن أبرز التحديات التي رافقت ظهور وانتشار نظم المعلومات المحاسبية الإلكترونية (EAIS) في بيئة تتسم بالمنافسة الشديدة ارتفاع المخاطر المرتبطة بأمن المعلومات الالكتروني والذي استدعى اهتمام إدارة الشركات به من حيث تطبيق إجراءات رقابة داخلية فعالة للمحافظة على أمن المعلومات داخل الشركة أو اكتشاف حالات تسريب المعلومات للأشخاص غير المصرح لهم.

1-2 مشكلة الدراسة وأسئلتها:

أدى انتشار أنظمة المعلومات المحاسبية الإلكترونية مع كل ما تحتويه من إيجابيات إلى ظُهور مخاطر حديثة لم تكن معروفة في السابق في النظام الورقي ومنها أمن نظم المعلومات الإلكترونية والمرتبط بإمكانية سرقة المعلومات والبيانات أو فقدانها أو تعديلها من خلال أفراد من خارج المنظمة أو من خلال الأفراد المستخدمين للنظام بالإضافة لإمكانية إطِّلاع المبرمجين على كافة البيانات المخزنة ضمن قواعد بيانات.

وبناءً على ذلك فإن مشكلة الدراسة يمكن تلخيصها في عدم توفر المعرفة الكافية عن مدى احتواء أنظمة المعلومات المحاسبية في الشركات الصناعية الأردنية على وسائل وأدوات لمنع و اكتشاف الأساليب المختلفة للاحتيال الإلكتروني المرتبطة بأمن المعلومات المحاسبية الإلكترونية والإجراءات اللازمة لتصحيح ثغرات النظام.

واستناداً لما ذكر آنفا يمكن إظهار مشكلة الدراسة بصورة أكثر وضوحا من خلال الأسئلة التالية:

1- ما مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية في منع الاحتيال الإلكتروني المرتبط بأمن المعلومات قبل حدوثه؟

2- ما مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية في اكتشاف الاحتيال الإلكتروني المرتبط بأمن المعلومات بعد حدوثه؟

3- ما مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات؟

4- ما هي المعوقات التي تؤثر على فاعلية إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية في الشركات الصناعية الأردنية؟

5- هل يوجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية (العمر، الدور الوظيفي الحالي، الرتبة الوظيفية، المؤهل العلمي، عدد سنوات الخبرة، الحصول على شهادات مهنية، تصنيف الشركة، عدد الموظفين، نوع الشركة) لكل منهم؟

1-3 فرضيات الدراسة:

تنطلق فرضيات الدراسة من محاولة الإجابة عن الأسئلة التي وردت في مشكلة الدراسة، وعلى النحو التالي:

الفرضية الأولى:

HO_1: لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني المرتبط بأمن المعلومات قبل حدوثه، ويتفرع عن هذه الفرضية الفرضيات الفرعية التالية:

1- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني الخاص باختراق الشبكات الحاسوبية (Hacking) قبل حدوثه.

2- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني الخاص بالهندسة الاجتماعية (Social Engineering) قبل حدوثه.

3- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني الخاص بالبرمجيات الضارة (Malware) قبل حدوثه.

الفرضية الثانية:

HO_2: لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في اكتشاف الاحتيال الإلكتروني المرتبط بأمن المعلومات بعد حدوثه، ويتفرع عن هذه الفرضية الفرضيات الفرعية التالية:

1- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في اكتشاف الاحتيال الإلكتروني من خلال اختراق الشبكات (Hacking) والمرتبط بأمن المعلومات بعد حدوثه.

2- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في اكتشاف الاحتيال الإلكتروني من خلال الهندسة الاجتماعية (Social Engineering) والمرتبط بأمن المعلومات بعد حدوثه.

3- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في اكتشاف الاحتيال الإلكتروني من خلال البرمجيات الضارة (Malware) والمرتبط بأمن المعلومات بعد حدوثه.

الفرضية الثالثة:

HO3: لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات، ويتفرع عن هذه الفرضية الفرضيات الفرعية التالية:

1- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات عن طريق اختراق الشبكات الحاسوبية (Hacking).

2- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات عن طريق الهندسة الاجتماعية (Social Engineering).

3- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات عن طريق البرمجيات الضارة (Malware).

الفرضية الرابعة:

HO4: لا توجد معوقات تؤثر على فاعلية إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية في الشركات الصناعية الأردنية.

الفرضية الخامسة:

HO5: لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم، ويتفرع عن هذه الفرضية الفرضيات الفرعية التالية:

1- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للعمر.

2- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للدور الوظيفي الحالي.

3- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للرتبة الوظيفية.

4- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للمؤهل العلمي.

5- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد سنوات الخبرة.

6- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للحصول على شهادات مهنية.

7- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لتصنيف الشركة.

8- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد الموظفين في الشركة.

9- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لنوع الشركة.

1-4 أهداف الدراسة:

يتمثل الهدف الرئيسي للدراسة في السعي لاكتشاف مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية المستخدمة لنظم المعلومات المحاسبية الإلكترونية في تخفيض

مخاطر أمن المعلومات لديها والمعوقات التي تؤثر على فاعلية هذه الإجراءات، ويمكن تقسيم هذا الهدف إلى الأهداف التالية:

1- بيان مدى فاعلية إجراءات الرقابة الداخلية في منع الاحتيال الإلكتروني المتعلق بأمن المعلومات قبل أن يحدث.

2- بيان مدى فاعلية إجراءات الرقابة الداخلية في اكتشاف الاحتيال الإلكتروني المتعلق بأمن المعلومات بعد أن يحدث.

3- بيان مدى فاعلية إجراءات الرقابة الداخلية في تصحيح ثغرات النظام التي تسببت بالاحتيال الإلكتروني المتعلق بأمن المعلومات.

4- بيان المعوقات التي تؤثر على فاعلية إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية.

5- بيان وجود فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم.

1-5 أهمية الدراسة:

تنبع الأهمية النظرية للدراسة من أهمية المحافظة على أمن المعلومات والبيانات الخاصة بالشركات الصناعية الأردنية وحمايتها من احتمال فقدانها، مما لها من تأثير على إستراتيجيتها وخططها المستقبلية وبالتالي نموها وتطورها في القطاع التي تنتمي إليه.

لقد واجهت بعض الشركات في الواقع العملي مشاكل بسبب ضعف نظام أمن المعلومات الإلكترونية لديها مما أدى إلى اختراق بياناتها والاحتيال عليها أو إتلاف بياناتها وبالتالي تكبدها خسائر مالية كبيرة لتعويض هذا الأمر.

وفي الأردن فإن بعض الشركات قد تعاني من ضعف في توفير متطلبات الرقابة على أمن معلوماتها نظراً لضعف أنظمتها للرقابة الداخلية، ومن هنا تأتي هذه الدراسة لتسهم في اكتشاف واقع هذا الأمر في الشركات الصناعية الأردنية، ويؤمل أن تؤدي هذه الدراسة إلى تقديم نتائج وتوصيات مفيدة للشركات الصناعية الأردنية تساهم في تحديد بعض نقاط الضعف ضمن مكونات نظم المعلومات المحاسبية الإلكترونية للمحافظة على أمن معلوماتها وسبل معالجتها.

1-6 حدود الدراسة:

اقتصرت الدراسة على الشركات الصناعية الأردنية التي تقوم بتطبيق نظم المعلومات المحاسبية.

1-7 التعريفات الإجرائية:

- **نظام المعلومات المحاسبي (Accounting Information System):**

هو النظام الذي يتم من خلاله التسجيل والمعالجة والتقرير عن الأحداث باستخدام الأساليب المحاسبية لتحقيق الأهداف المحاسبية. (Boockholdt, 1999)

- **أمن المعلومات (Information Security):**

هي درجة الثقة بالأمن والحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام. (Raval & Fichadia, 2007)

- **الرقابة الداخلية (Internal Control):**

هي عمليه تتأثر بمجلس إدارة المنظمة وإدارتها وأفراد آخرين، صممت لتوفير تأكيد معقول لضمان تحقيق الأهداف المتعلقة بالرقابة على كفاءة وفاعلية العمليات وموثوقية القوائم المالية والتأكد من الامتثال للقوانين والأنظمة والسياسات ذات العلاقة بالمنظمة. (Committee of Sponsoring Organizations - COSO, 1994)

- **أنشطة الرقابة (Control Activities):**

هي تصميم وتنفيذ مجموعة من السياسات والإجراءات لضمان الاستجابة الفعالة للمخاطر. (Committee of Sponsoring Organizations - COSO, 1994)

- **إجراءات منع الاحتيال الإلكتروني (Prevention procedures for electronic fraud):**

هي الإجراءات التي تهدف لمنع سرقة أو تعديل أو اتلاف البيانات المدخلة من خلال نظم المعلومات المحاسبية الإلكترونية والمخزنة ضمن قواعد البيانات.

- **إجراءات اكتشاف الاحتيال الإلكتروني (Detection procedures for electronic fraud):**

هي الإجراءات التي من شأنها اكتشاف سرقة البيانات والمعلومات أو تعديلها أو اتلافها والمدخلة من خلال نظم المعلومات المحاسبية الإلكترونية والمحفوظة ضمن قواعد البيانات.

- **إجراءات تصحيح الاحتيال الإلكتروني (Correction procedures for electronic fraud):**

هي الإجراءات التي تهدف لمعالجة الثغرات ضمن مكونات نظم المعلومات المحاسبية وذلك لمنع تكرار سرقة البيانات والمعلومات أو تعديلها أو اتلافها والتي تم إدخالها من خلال نظم المعلومات المحاسبية الإلكترونية.

- **الشبكة (Network):**

هي مجموعة من الأجهزة المرتبطة معاً من خلال قنوات الاتصال السلكية و/أو اللاسلكية (Raval & Fichadia, 2007)

- **اختراق الشبكات (Hacking):**

وهو الوصول غير المصرح به للشبكة الحاسوبية أو نظام المعلومات المحاسبي بهدف تعديل البيانات و المعلومات أو سرقتها أو تدميرها. (Romney & Steinbart, 2012)

- **الهندسة الاجتماعية (Social Engineering):**

تحفيز مستخدم الحاسوب على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة أي شبهة. (Romney & Steinbart, 2012)

- **البرمجيات الضارة (Malware):**

وهي البرامج المتخصصة بتسهيل التسلل إلى النظام أو الشبكة الحاسوبية بهدف تدميره، وما أن يتم تثبيت البرمجية الضارة فإنه من الصعب جداً إزالتها. (Romney & Steinbart, 2012)

الفصل الثاني

الإطار النظري والدراسات السابقة

الفصل الثاني

الإطار النظري والدراسات السابقة

2-1 المقدمة

2-2 الرقابة الداخلية

2-3 نظم المعلومات المحاسبية الإلكترونية

2-4 أمن المعلومات

2-5 الدراسات السابقة

2-6 ما يميز هذه الدراسة عن الدراسات السابقة

2-1 المقدمة:

لعل واحدة من أهم حقائق الأعمال المتعارف عليها أن نظم المعلومات المحاسبية تشكل إحدى الأدوات المهمة للتقرير عن أنشطة وربحية منظمات الأعمال. وإذا كان استخدام تكنولوجيا المعلومات قد أحدث تحولاً في نظم المعلومات المحاسبية الورقية (Paper-Based AIS) باتجاه نظم المعلومات المحاسبية القائمة على استخدام الحاسوب (Computer-Based AIS)، فإن أهمية توظيف تكنولوجيا المعلومات واستخدامها في بنية نظم المعلومات المحاسبية تتأتى من كونها مكّنت من إعادة تصميم نظم الرقابة الداخلية المحاسبية باتجاه ضمان كفاءة تشغيلية أكبر من ناحية، وموضوعية أداء أوثق من ناحية أخرى. (مشتهى و حمدان و شكر، 2011، ص 21)

ويرى (الرمحي والذيبة، 2011) أن نظام المعلومات المحاسبي يقدم معلومات دقيقة باعتباره نظام دعم، وهذا يمّكن عناصر سلسلة القيمة من تأدية وظائفها وأنشطتها بشكل فعال، حيث يتمكن هذا النظام من تحقيق ذلك من خلال تحسين الإنتاجية وزيادة الكفاءة والفاعلية من خلال تقديم معلومات دقيقة والمشاركة في المعرفة من خلال مشاركة عدد كبير من الموظفين في المعلومات من مكاتب عدة في مؤسسة واحدة وتحسين القدرة على اتخاذ القرار.

تقوم الشركات التي تعمل في العالم الإلكتروني بتخزين البيانات والمعلومات الحساسة في أجهزة الحاسوب المتصلة بالشبكات، وقد تكون هذه الشبكات عرضة للاختراق وبالتالي قد تؤدي لتلف البيانات، وبناءً عليه يجب أن يكون أمن المعلومات أهم جزء في تطبيقات الأعمال. (Smith, 2009)

2-2 الرقابة الداخلية:

تعتبر الرقابة الداخلية في الشركات الصناعية جزءاً هاماً من عملياتها، حيث يؤدي تطبيق نظام رقابة داخلية قوي لحصول المنظمة على فوائد عديدة منها:

1- تخفيض كلفة التدقيق الخارجي من خلال انخفاض مخاطر التدقيق.

2- تمكين المنظمة من السيطرة بشكل فعال على أصول الشركة.

3- زيادة الملاءمة والموثوقية للمعلومات المستخدمة لاتخاذ القرار.

بينما يؤدي نظام رقابة داخلية ضعيف إلى وضع الشركات الصناعية في مخاطر عديدة منها إتاحة الفرصة لسرقة الأصول من قبل الموظفين، واحتمالية فقدان المعلومات المتعلقة بالعمليات، وغيرها من المخاطر والتهديدات التي قد تؤدي إلى فشل منظمات الأعمال في تحقيق أهدافها.

2-2-1 تعريف الرقابة الداخلية وأهدافها:

تم تعريف الرقابة الداخلية من قبل لجنة تمويل المنظمات (Committee of Sponsoring Organizations - COSO) ضمن الأطار المتكامل للرقابة الداخلية (Internal Control integration Framework) والمنشور في عام 1994، بأنها عملية تتأثر بمجلس إدارة المنظمة وإدارتها وأفراد آخرين، صممت لتوفير تأكيد معقول يضمن تحقيق الأهداف التالية: (COSO, 1994)

1- كفاءة وفاعلية العمليات (Effectiveness and Efficiency of Operations).

2- موثوقية القوائم المالية (Reliability of Financial Reporting).

3- الامتثال للقوانين والتشريعات ذات العلاقة بالمنظمة (Compliance with applicable laws and regulations).

2-2-2 مكونات الرقابة الداخلية:

لقد حددت لجنة تمويل المنظمات (COSO) ضمن الإطار المتكامل للرقابة الداخلية خمسة عناصر مترابطة للرقابة الداخلية وهي:

1- بيئة الرقابة (Control Environment):

تتكون بيئة الرقابة الداخلية من مجموعة من سياسات وإجراءات وأفعال تعكس سلوك المدراء والإدارة العليا والمالكين تجاه الرقابة الداخلية وأهميتها للشركة. (Elder, Beasley & Arens, 2010)

2- تقييم المخاطر (Risk Assessment):

تواجه الشركات مخاطر متعددة من عدة مصادر داخلية مثل طبيعة أنشطة المنشأة، وخارجية مثل التطورات التكنولوجية والأوضاع الاقتصادية، ويجب على المنظمة تحديد هذه المخاطر وكيفية التعامل معها، وهنا يتم التركيز على كل من احتمالية حدوث الخطر والأثر المادي المتوقع له والتخطيط في ضوء ذلك، ولذلك يجب على المنظمة وضع آلية لتحديد وتحليل وإدارة المخاطر التي قد تواجهها.

3- أنشطة الرقابة (Control Activities):

هي الإجراءات التي توضع من أجل الرقابة الداخلية وتحقيق أهداف المنظمة ومنها فصل المهام وتفويض الصلاحيات بشكل مناسب والاحتفاظ بالسجلات والوثائق والرقابة المادية على السجلات والأصول. (Soltani, 2007)

4- المعلومات والاتصال (Information & Communication):

وجود نظام للمعلومات والاتصال يمكن الأشخاص العاملين في المنظمة من التقاط وتبادل المعلومات اللازمة لإجراء وإدارة ومراقبة عملياتها. (COSO, 1994)

حيث تؤثر جودة المعلومات التي يتم الحصول عليها من خلال نظام المعلومات المحاسبي في قدرة الادارة على اتخاذ القرارات المناسبة فيما يتعلق بالرقابة على أنشطة المنظمة وإعداد قوائم مالية يمكن الاعتماد عليها. (Hayes et al, 2005)

5-المراقبة (Monitoring):

يجب على الإدارة متابعة نظام الرقابة الداخلية، حيث يمكن تقييم جودة أداء نظام الرقابة الداخلية من خلال مراقبته بشكل مستمر. (COSO, 1994)

ومن المعلومات التي يمكن الاستفادة منها في هذا الإطار تقرير المدقق الداخلي والمعلومات الواردة من الموظفين التشغيليين (Porter, Simon & Hatherly,2008) ومن الزبائن (Hayes et al, 2005)

2-3 نظم المعلومات المحاسبية الإلكترونية:

2-3-1 تعريف نظام المعلومات المحاسبي:

يمكن تعريف نظام المعلومات المحاسبي بأنه نظام يتم من خلاله جمع البيانات ومعالجتها للحصول على معلومات مفيدة لمتخذي القرار (Bagranoff , Simkin & Norman, 2005)، كذلك تم تعريفه بأنه نظام يتم من خلاله تجميع وتسجيل وتخزين ومعالجة البيانات في سبيل الحصول على معلومات لمتخذي القرار، كما يتم من خلاله حماية أصول المنشأة بما فيها البيانات. (Romney & Steinbart, 2012).

كذلك تم تعريف نظام المعلومات المحاسبي بأنه النظام الذي يتم من خلاله التسجيل والمعالجة والتقرير عن الأحداث باستخدام الأساليب المحاسبية لتحقيق الأهداف المحاسبية. (Boockholdt, 1999)

2-3-2 مكونات نظام المعلومات المحاسبي:

قد يكون نظام المعلومات المحاسبي بسيطاً جداً من خلال تطبيق النظام اليدوي، أو أن يكون معقدا من خلال تطبيق آخر ما توصلت إليه التكنولوجيا، ويمكن أن يكون بين هذين المستويين. (Romney & Steinbart, 2012)

إن نظم المعلومات المحاسبية كغيرها من الأنظمة الأخرى لها مكونات خاصة بها تسهل عليها عملية القيام بالوظائف والأهداف التي وضعت من أجلها، ويمكن توضيح هذه المكونات والوظائف التي تدعمها كالتالي : (Romney & Steinbart, 2012)

1- المصادر البشرية التي تقوم باستخدام هذا النظام وتؤدي من خلاله وظائف مختلفة.

2- التعليمات والإجراءات اليدوية والإلكترونية التي تستخدم في تجميع ومعالجة وحفظ وإيصال المعلومات حول أنشطة المنظمة.

3- البيانات حول المنظمة وأسلوب عملها.

4- البرامج المستخدمة في معالجة بيانات المنظمة.

5- البنية التحتية لتكنولوجيا المعلومات والتي تشمل أجهزة الحاسوب، الأجهزة الطرفية، وشبكة الاتصالات التي تجمع وتحفظ وتعالج البيانات والمعلومات.

6- التدقيق الداخلي ومقاييس الأمن، والتي تضمن أمن البيانات في نظام المعلومات المحاسبي.

وتمكن هذه المكونات الستة نظام المعلومات المحاسبي من تلبية ثلاث وظائف مهمة للمنظمة وهي: (Romney & Steinbart, 2012)

1- جمع وحفظ المعلومات عن نشاطات وموارد المنظمة.

2- تحويل البيانات إلى معلومات مفيدة لصناعة القرار، وهذا يُمكن الإدارة من التخطيط والرقابة، وتقييم النشاطات والموارد والموظفين.

3- تقديم رقابة كفؤة للمحافظة على أصول المنظمة بما في ذلك المعلومات للتأكد من توفرها عند الحاجة وأن البيانات دقيقة وموثوقة.

2-4 أمن المعلومات:

2-4-1 تعريف أمن المعلومات:

مصطلح الأمن (Security) يعني ضمناً الحماية (Protection)، ويعتمد هذا المفهوم على السياق الذي ذكر فيه، وهو في هذه الدراسة أمن نظم المعلومات المحاسبية. أيضا غالبا ما يشير هذا المصطلح للثقة (Confidence) أو لمستوى الراحة المرتبطة بالأمن والحماية من الضرر الناتج عن المخاطر، بالإضافة لذلك فإن الأضرار المحتملة تأتي من التهديدات التي تستغل ثغرات أو ضعف النظام (System's Vulnerability). بناءً على ما سبق يمكن تعريف أمن المعلومات بأنها درجة الثقة بالأمن والحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام. (Raval & Fichadia, 2007)

2-4-2 أهداف أمن المعلومات:

الهدف الرئيسي من أمن المعلومات هو حماية نظام المعلومات بالشركة ومكوناته، بناءً على ذلك فإن السبب الرئيسي لأمن الأصول المعلوماتية هو التأكد من عدم تعرضها للمخاطر وأنها متاحة للأشخاص المصرح لهم. (Raval & Fichadia, 2007)

بناءً على ما تقدم فإن أهداف أمن المعلومات تتلخص بما يلي: (Raval & Fichadia, 2007)

1- نزاهة المعلومات (Information Integrity): تكون المعلومات نزيهة عندما تكون المعلومات المستخرجة من النظام دقيقة وموثوقة.

2- السرية (Confidentiality): يجب الإحتفاظ بالمعلومات السرية بعيداً عن الأشخاص غير المصرح لهم.

3- التحقق من المستخدم (User Authentication): هي عملية المصادقة على هوية الأشخاص المصرح لهم.

ولتحقيق أهداف أمن المعلومات المشار إليها أعلاه، يرى الباحث ضرورة أن يكون لدى الإدارة العليا بالشركات الصناعية الأردنية والمحاسبين والمدققين الداخليين معرفة جيدة بآلية عمل نظم المعلومات المحاسبية الإلكترونية (EAIS) والتأكد من احتوائها على متطلبات الرقابة الداخلية بشكل عام وكيفية المحافظة على سرية البيانات والمعلومات المخزنة ضمن قواعد البيانات بشكل خاص.

2-4-3 الرقابة على أمن المعلومات:

تعتبر الرقابة على أمن المعلومات من المواضيع الهامة والتي يجب الاهتمام بها من قبل الإدارة العليا نظراً للأهمية الإستراتيجية التي تتمتع بها إذ إن هناك سببين رئيسين للمحافظة على المعلومات داخل الشركة وهما: (Raval & Fichadia, 2007)

1- احتمالية اختراق الأنظمة وسرقة المعلومات والبيانات منها أو تعديلها بشكل غير مرغوب أو أن يتم تعديلها من قبل مستخدمي النظام بشكل مقصود أو غير مقصود.

2- الامتثال لمتطلبات قوانين الحماية والخصوصية، وعلى سبيل المثال يجب المحافظة على خصوصية المعلومات المتعلقة بالموظفين والزبائن والموردين... الخ. إذ إن أي انتهاك لهذه القوانين يمكن أن تؤدي إلى نتائج سلبية تؤثر على الموقف القانوني للشركة وسمعتها.

2-4-3-1 الرقابة الوقائية:

تحتوي الرقابة الوقائية على ضوابط تهدف لمنع وقوع الأحداث السلبية والخسائر في الأصول والموارد، ومن أمثلة هذه الضوابط فصل المهام بين الوظائف الإدارية والعمليات وتوثيقها وتقييد الوصول لأصول وموارد المنشأة. (Boczko, 2012)

بناءً على ما سبق يمكن تعريف الرقابة الوقائية بأنها الرقابة المعنية بمنع حدوث الخطر، وتتضمن الوظائف التالية: (Romney & Steinbart, 2012)

أ- **التدريب (Training):**

يجب أن يتم تدريب الموظفين على الممارسات الآمنة عند استخدام الحاسوب، ومنها عدم فتح الملفات المرفقة بالبريد الإلكتروني مجهول المصدر، وحصر استخدام البرامج بالمرخصة فقط

والاحتفاظ بكلمة السر وعدم الإفصاح عنها لأي شخص، والاحتفاظ بالحاسوب المحمول بمكان آمن وخصوصاً خلال السفر. (Romney & Steinbart, 2012)

ب- الرقابة على تصريح الدخول (User Access Controls):

ويمكن تقسيمها إلى وظيفتين رئيسيتين هما: أولاً التحقق (Authentication): أي التأكد من هوية الشخص أو الجهاز الذي يقوم بالولوج للنظام، وثانياً التصريح (Authorization): أي حصر الولوج للنظام أو جزء منه بالأشخاص المخولين وتحديد الصلاحيات لكل شخص مستخدم. (Romney & Steinbart, 2012)

أولاً: التحقق (Authentication):

ويتم التحقق من المصادقة إما من خلال شيء يتم معرفته مثل كلمة السر التي تعتبر الأكثر شيوعاً في مثل هذا المجال، أو رقم التعريف الشخصي، أو من خلال شيء يتم امتلاكه مثل البطاقات الذكية أو بطاقات تعريف الشخصية، أو عن طريق بعض الخصائص المادية مثل بصمة الإصبع أو الصوت. (Romney & Steinbart, 2012)

ثانياً: التصريح (Authorization):

ويتم تطبيقها من خلال إنشاء مصفوفة صلاحيات الدخول، وهي عبارة عن جدول يحدد صلاحيات مستخدمي النظام. (Romney & Steinbart, 2012)

يتمثل التحقق (Authentication) و التصريح (Authorization) بسياسات الشركة الخاصة بتقييد الولوج للنظام، وتقييد العمليات التي يمكن تنفيذها من قبل مستخدمي النظام وحسب الصلاحيات المعتمدة لكل مستخدم. حيث يجب عمل اختبار لتقييم التوافق مع هذه السياسات من خلال تحليل سجل استخدام النظام (Log Analysis)، بالإضافة لذلك، فمن المهم إجراء اختبار دوري لتقييم كفاءة إجراءات الأمن المطبقة في الشركة. إذ يقوم النظام بتنفيذ اختبار التوافق

(Compatibility Test) من خلال مطابقة مصادقة المستخدم Authentication (Credential) مع مصفوفة الصلاحيات، وبالتالي تنظيم دخول المستخدمين للنظام كلٌ حسب صلاحياته. (Romney & Steinbart, 2012)

ج- الرقابة على الوصول المادي (Controlling Physical Access):

ويقصد منها منع الوصول المادي وحماية مكونات نظم المعلومات المحاسبية من أجهزة وبرمجيات وبنية تحتية، وذلك من خلال حصر الوصول لهذه المكونات بالأشخاص المصرح لهم بذلك وحمايتها من التلف من خلال تزويد مبنى الشركة بأنظمة إطفاء الحريق مثلاً. (Romney & Steinbart, 2012)

د- الرقابة على الوصول إلى الشبكة الحاسوبية (Network Access Controls):

تخضع المعلومات المرسلة من خلال الإنترنت إلى نوعين من البروتوكولات وهما برتوكولات التحكم بالإرسال (Transmission Control Protocol - TCP)، والذي يعمل من خلال تحديد الإجراءات لتقسيم الملفات والوثائق إلى حزم وإعادة تجميعها عند وصولها لوجهتها. أما البروتوكول الآخر فهو برتوكول الإنترنت (Internet Protocol - IP) وهو الذي يحدد هيكلة الحزم وكيفية وصولها إلى وجهتها الصحيحة، إذ تتكون كل حزمة من حزم بروتوكول الإنترنت (IP) من جزأين هما العنوان (Header) والذي يحتوي على عنوان مرسل الحزمة وعنوان الجهة المستقبلة لها، والهيكل (Body) والذي يحتوي على معلومات حول نوع المعلومات المرسلة، إذ يتم إرسال البيانات من خلال أجهزة لتحديد الوجهات (Routers) وذلك من خلال قراءة حقل عنوان الجهة المستقبلة الموجود في جزء العنوان (Header) لتحديد الطريق الذي سيتم إرسال الحزمة التالية من خلاله. وتتم حماية شبكة الحاسوب من الرسائل غير المرغوبة من خلال عدة وسائل منها الجدار الناري (Firewall) وذلك من خلال

فلترة الحزم والسماح لمرور الحزم التي تلبي شروط معينة فقط. (Romney & Steinbart, 2012)

هـ- توفير الأمن والحماية للأجهزة والبرمجيات:

يتعزز أمن المعلومات من خلال استكمال الضوابط الوقائية في محيط الشبكة مع الضوابط الوقائية الإضافية على محطات العمل والخادم والطابعات والأجهزة الأخرى التي تشكل شبكة المنظمة. (Romney & Steinbart, 2012)

2-4-3-2 الرقابة الاكتشافية:

يتم تنفيذ هذا النوع من الرقابة على الأحداث بعد حصولها، إذ أنها تصمم لاكتشاف الأحداث التي تحتوي على نتائج غير مرغوب فيها والتي قد تكون حصلت فعلاً. (Boczko, 2012)

وكما هو معروف، فمن غير الممكن منع المخاطر قبل حدوثها بشكل قطعي، لذلك تحتاج الشركات بالإضافة للرقابة الوقائية إلى تطبيق رقابة مصممة لاكتشاف المخاطر عند حدوثها إذ تعمل الرقابة الاكتشافية على تحسين أمن النظام من خلال مراقبة كفاءة الرقابة الوقائية، واكتشاف التحايل على الرقابة الوقائية في حالة حدوثها إذ إن من الضروري توفر سجل دخول للنظام (Log File) مدون فيه مثلا اسم المستخدم والجهاز والوقت والتاريخ التي تمت فيه الحركة، بالإضافة إلى تحليل سجل الدخول لا بُد من اختبار النظام والتدقيق عليه بشكل دوري، وقد يتم ذلك من خلال أسلوب مسح الثغرات بواسطة برنامج خاص يتم تشغيله لتحديد ما إذا كان يوجد في النظام ثغرات أم لا. (Romney & Steinbart, 2012)

2-4-3-3 الرقابة التصحيحية:

يُصمم هذا النوع من الرقابة لعلاج أو لإصلاح الحالات التي تمت فعلاً لاختراق أنظمة الحماية من خلال التهديدات أو / و الأحداث غير المرغوبة. (Boczko, 2012)

يعتبر اكتشاف محاولات التحايل سواء الناجحة أو غير الناجحة مهم جداً، ولكن يفقد هذا الاكتشاف قيمته في حالة عدم إتباعه بإجراءات تصحيحية لضمان الحد من تكراره، ومن هذه الإجراءات إنشاء فريق استجابة للتهديدات التي يتعرض لها النظام بالإضافة لتعيين مدير تنفيذي لأمن المعلومات بحيث يكون من واجباته تقييم البيئة التي يعمل فيها النظام بالإضافة لتحليل وتقييم ثغرات النظام، وأخيراً من الضروري تحديث البرامج ذات العلاقة بشكل دوري مثل البرامج المضادة للفيروسات والجدار الناري وأنظمة التشغيل والتطبيقات. (Romney & Steinbart, 2012)

2-4-4 التهديدات التي تواجه أمن المعلومات:

تتزايد التهديدات التي تتعرض لها المنظمات نتيجة التطور المتسارع في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصة بالمنظمة بشكل غير مصرح به بهدف تعديلها أو سرقتها أو حتى تدميرها.

يمكن تصنيف أساليب الاحتيال الإلكتروني بهدف الحصول على المعلومات بأسلوب غير مصرح به إلى ثلاثة أساليب وهي: (Romney & Steinbart, 2012)

أ- اختراق الشبكات (Hacking):

ويقصد به الوصول غير المصرح به للشبكة أو نظام المعلومات المحاسبي بهدف تعديل البيانات أو المعلومات أو سرقتها أو تدميرها، ويحتوي هذا الأسلوب على عدة

تِقنيات منها التالية التي تم اختيارها في أداة الدراسة كأمثلة على تقنيات شائعة جداً في هذا المجال : (Romney & Steinbart, 2012)

1- سرقة كلمة السر (Password cracking)، اختراق الشبكة والإطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة.

2- التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack).

3- هجمات حقن قواعد البيانات (Structured Query Language Injection Attack)، مثلاً من خلال إدخال برمجية ضارة مكان كلمة السر أو اسم المستخدم إذ تمكن المحتال من الوصول إلى قواعد البيانات بهدف سرقتها أو التعديل فيها أو تدميرها.

ب-الهندسة الاجتماعية (Social Engineering):

ويقصد بها تحفيز المستخدم على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة أي شبهة، ويحتوي هذا الأسلوب على عدة تِقنيات منها التالية التي تم اختيارها في أداة الدراسة كأمثلة على تقنيات شائعة جداً في هذا المجال:

1- التوأمة الشريرة (Evil Twin)، أي إدعاء جهة معينة بأنها جهة موثوق منها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به.

2- سرقة الهوية (Identity theft)، أي إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر.

3- التصيد (Phishing)، ويقصد منها وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة.

ج- البرمجيات الضارة (Malware):

وهي عبارة عن برامج متخصصة لتسهيل التسلل إلى النظام أو الشبكة بهدف تدميرها، وما أن يتم تثبيت البرمجية الضارة فإنه من الصعب جداً إزالتها، ويحتوي هذا الأسلوب على عدة تِقنيات منها التالية التي تم اختيارها في أداة الدراسة كأمثلة على تقنيات شائعة جداً في هذا المجال:

1- حصان طروادة (Trojan Horse)، وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال.

2- الفيروسات (Viruses)، وهي برامج تدخل إلى الحاسوب ويتصل بالملفات المخزنة به ثم يكرر نفسه بحيث يتم تدمير هذه الملفات.

3- برامج التجسس (Spyware)، وهي البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت.

2-5 الدراسات السابقة:

فيما يلي عرض للدراسات السابقة والمتعلقة بالموضوع وذات العلاقة:

1- دراسة Fulford & Doherty (2003) بعنوان "The application of information security policies in large UK-based organizations: an exploratory investigation"

هدفت الدراسة إلى البحث في استيعاب ونشر أثر سياسات أمن المعلومات في الشركات الكبيرة في المملكة المتحدة، وخلصت إلى أنه على الرغم من شيوع سياسات امن المعلومات إلا انه لا تزال فيها درجة عالية من التنوع من حيث محتواها ونشرها.

2-دراسة القشي، (2003) بعنوان "مدى فاعلية نظم المعلومات المحاسبية في تحقيق الأمان والتوكيدية والموثوقية في ظل التجارة الالكترونية"

هدفت الدراسة إلى التعرف على المشاكل التي تواجه أنظمة المعلومات المحاسبية في ظل استخدام التجارة الإلكترونية، وتطوير نموذج للربط بين هذه الأنظمة والتجارة الإلكترونية.

وقد توصلت الدراسة إلى أن التجارة الإلكترونية أثَّرت على جميع المجالات المهنية بشكل عام وعلى مهنتي المحاسبة والتدقيق بشكل خاص، و أنها تعمل في بيئة فريدة من نوعها بحيث أن العمليات التي تتم من خلالها عمليات غير ملموسة تفتقد لآلية التوثيق في أغلب مراحلها، مما يسهم بشكل مباشر في إيجاد مشكلتين رئيسيتين واجهتا مهنتي المحاسبة والتدقيق و هما آلية التحقق والاعتراف بالإيراد المتولد من عمليات التجارة الإلكترونية و آلية تخصيص الضرائب على مبيعات وإيرادات عمليات التجارة الإلكترونية. و أوصت الدراسة بتوفير سياسات و إجراءات عملية

تساهم في تحقيق الأمان والموثوقية لمخرجات النظام المحاسبي المتعامل بالتجارة الإلكترونية، و إنشاء وتطوير نظام ربط بين نظام الشركة المحاسبي وموقعها الإلكتروني على شبكة الانترنيت.

3- دراسة Gupta & Hammond (2005) بعنوان "Information systems security issues and decisions for small businesses: an empirical examination"

هدفت الرسالة لجمع معلومات عن تكنولوجيا المعلومات والمتعلقة بأمن المعلومات للشركات الصغيرة في قطاعي الخدمات والشركات الصناعية، وخلصت الدراسة إلى أنه من الممكن أن تمتلك الشركات الصغيرة سياسات وإجراءات لمواجهة المخاطر المتعلقة بأمن المعلومات وأن تطبق تقنيات لذلك و لكنها غير فعالة.

4- دراسة Hayale & Abu Khadra (2006) بعنوان "Evaluation of the effectiveness of control systems in computerized accounting information systems: An empirical research applied on Jordanian banking sector "

هدفت الدراسة لتقييم درجة فاعلية نظام الرقابة الداخلية على نظم المعلومات المحاسبية المحوسبة في قطاع البنوك الأردنية للمحافظة على سرية ونزاهة بيانات البنوك وإتاحتها. وخلصت الدراسة إلى أن البنوك الأردنية تطبق نظام رقابة فعال لتقليل حوادث الاحتيال والخطأ الإلكتروني لكنها تفتقد إلى نظم رقابية أخرى مثل الوصول المادي والمنطقي للأنظمة وأمن المعلومات، وخطط الطوارئ، والإنترنت، وعلى الاتصال الالكتروني وأخيرا على مخرجات الرقابة.

5- دراسة البحيصي و الشريف، (2008) بعنوان "مخاطر نظم المعلومات المحاسبية الإلكترونية :دراسة تطبيقية على المصارف العاملة في قطاع غزة"

هدفت هذه الدراسة للتعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، و أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر.

و من نتائج الدراسة أن حدوث مخاطر نظم المعلومات المحاسبية الالكترونية يرجع إلى موظفي البنك بسبب قلة الخبرة والوعي والتدريب، كما يرجع إلى إدارة المصرف بسبب عدم وجود سياسات واضحة ومكتوبة وضعف الاجراءات الرقابية.

6- دراسة الحسبان، (2008) بعنوان "مدى مواكبة المدققين الداخليين لمتطلبات تكنولوجيا معلومات أنظمة الرقابة الداخلية في الشركات المساهمة العامة الأردنية"

غطت هذه الدراسة المدققين الداخليين في الشركات المساهمة العامة المدرجة في بورصة عمان للأوراق المالية، في السوق الأول والثاني فقط، و توصلت الى أن هناك تأثير لبيئة تكنولوجيا المعلومات على نظام الرقابة الداخلية، حيث أنه عند تكوين بيئة الرقابة في ظل بيئة تكنولوجيا المعلومات يؤدي ذلك الى تعيين مجلس إدارة ولجنة تدقيق أكثر خبرة ودراية بأنظمة بيئة تكنولوجيا الرقابة، كما يراعى تحديد الصلاحيات والمسؤوليات لكل موظف من ذوي العلاقة ببيئة تكنولوجيا المعلومات.

7- دراسة الحكيم، (2010) بعنوان "إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمته للمؤسسات العامة ذات الطابع الاقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية"

غطت الدراسة إمكانية القيام بتقييم بنية الرقابة الداخلية المؤتمتة من قبل مفتشي الجهاز المركزي للرقابة المالية عند قيامهم بعملية التدقيق على المؤسسات التي تستخدم نظم المعلومات المحاسبية المؤتمتة وفق معايير الرقابة على نظم المعلومات.

ومن نتائج الدراسة أنه لا توجد فروق ذات دلالة إحصائية تعبر عن ازدياد الفاعلية الرقابية على تقنية المعلومات وذلك مع ازدياد استخدام الضوابط الرقابية المتعلقة وفق المعايير الرقابية المتعارف عليها، كما لا توجد فروق ذات دلالة إحصائية تعبر عن ازدياد الفاعلية الرقابية على تقنية المعلومات وذلك مع ازدياد استخدام إجراءات الرقابة من قبل المفتشين.

8- دراسة حمادة، (2010) بعنوان "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية (دراسة ميدانية)"

غطت هذه الدراسة الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية وأثرها في زيادة موثوقية المعلومات المحاسبية، وقد تم توزيع إستبانة على مكاتب التدقيق في دمشق تضمنت الضوابط الرقابية العامة الأربعة لنظم المعلومات المحاسبية الإلكترونية و هي الضوابط التنظيمية وضوابط الرقابة على الوصول وضوابط أمن وحماية الملفات وضوابط تطوير وتوثيق النظام. وخلصت الدراسة إلى أن للضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية لها تأثير كبير في زيادة موثوقية المعلومات المحاسبية في الشركات.

9- دراسة الرحاحلة، (2010) بعنوان "فاعلية متطلبات نظام الرقابة الداخلية على تكنولوجيا المعلومات في الوزارات والمؤسسات العامة الأردنية"

هدفت الدراسة إلى التعرف على فاعلية متطلبات نظام الرقابة الداخلية (القانونية والتشريعية، والحماية والأمن، والإدارية) على تكنولوجيا المعلومات في الوزارات والمؤسسات العامة الأردنية، وخلصت الدراسة إلى وجود فاعلية لمتطلبات نظام الرقابة الداخلية على تكنولوجيا المعلومات مجتمعة

10- دراسة Joo et al (2011) بعنوان "Determinants Of Information Security Affecting Adoption of Web-Based Integrated Information Systems"

هدفت الدراسة لتحليل العوامل المحددة لأمن المعلومات والتي تؤثر على درجة الاعتماد على نظم المعلومات المستندة على شبكة الإنترنت، وخلصت الدراسة إلى أن الرقابة الوقائية تلعب دوراً مهماً وفعالاً في أمن وحماية المعلومات وتقليل المخاطر المحتملة.

11- دراسة Hall , Sarkani & Mazzuchi (2011) بعنوان "Impacts of organizational capabilities in information security"

هدفت الدراسة لاختبار العلاقة بين استراتيجية أمن المعلومات وأداء الشركة مع قدرات الشركة كعامل مهم في انجاح تطبيق استراتيجية امن المعلومات و انجاح الشركة، وخلصت إلى وجود دلائل على أن قدرات المنظمة التي تشمل القدرة على تطوير وعي ظرفي عالي الجودة بالمخاطر البيئية الحالية و المستقبلية والقدرة على امتلاك الوسائل المناسبة والقدرة على تنظيم الاستجابة لمخاطر أمن المعلومات تنعكس إيجابيا على فاعلية تطبيق استراتيجية أمن المعلومات

والذي بدوره يؤثر إيجابيا على أداء المنظمة، ومع ذلك ليس هناك علاقة ذات دلالة إحصائية بين صنع القرار و نجاح تطبيق استراتيجية أمن المعلومات.

2-6 ما يميز هذه الدراسة عن الدراسات السابقة:

إن أهم ما يميز هذه الدراسة عن الدراسات السابقة، هو تركيزها على أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية باعتبارها أحد الأصول الإستراتيجية والمهمة لهذه الشركات في بيئة يتزايد فيها الاعتماد على نظم المعلومات المحاسبية في إدخال ومعالجة عملياتها اليومية، ونتيجة لانتشار هذه النظم أصبح اختراق أنظمة المعلومات المحاسبية خطراً يقلق العديد من الشركات في السنوات الأخيرة.

ويرى الباحث أنه كي يتم المحافظة على أمن المعلومات فيجب التركيز على إجراءات الرقابة الداخلية التي تساعد هذه الشركات في الحد من المخاطر التي تؤثر على سرية وأمن معلوماتها، والتي لن تتحقق من وجهة نظر الباحث سوى من خلال تصميم إجراءات رقابية فعالة ومتكاملة تقوم في البداية بتحديد وتقييم المخاطر المرتبطة بأمن المعلومات، تمهيدا لتطوير الإجراءات اللازمة لمنع سرقتها وفقدانها، والكشف عن سرقة أو فقدان هذه المعلومات إن حصل، وأخيرا مراجعة هذه الإجراءات بشكل دوري وعند الحاجة في سبيل تطويرها وتحسينها بشكل مستمر.

وما يميز هذه الدراسة عن سابقاتها أنها من الدراسات النادرة في الأردن (لا يوجد دراسة سابقة لها حسب علم الباحث) التي غطت المخاطر الإلكترونية وأنواعها وإجراءات الرقابة عليها بهذه الدرجة من التفصيل، وبالتالي فإنها تقدم إضافة علمية بارزة في مجال أمن المعلومات وأنظمة المعلومات المحاسبية والرقابة عليها في الشركات الصناعية الأردنية.

الفصل الثالث

الطريقة والإجراءات

الفصل الثالث

الطريقة والإجراءات

3-1 المقدمة

3-2 منهجية الدراسة

3-3 مجتمع الدراسة وعينتها

3-4 أداة الدراسة ومصادر الحصول على المعلومات

3-5 المعالجة الإحصائية المستخدمة

3-1 المقدمة:

يتمثل الهدف الرئيسي للدراسة في السعي لاكتشاف مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية المستخدمة لنظم المعلومات المحاسبية الإلكترونية في تخفيض مخاطر أمن المعلومات لديها والمعوقات التي تؤثر على فاعلية هذه الإجراءات، ولتحقيق هذا الهدف تم تصميم وتطوير أداة لاستطلاع آراء أفراد عينة الدراسة

سيتناول الباحث في هذا الفصل المنهجية المطبقة في إجراء هذه الدراسة و يستعرض أداة الدراسة وتفاصيلها وصدق وثبات أداة الدراسة والأساليب الإحصائية المستخدمة، وكذلك مجتمع الدراسة وعينتها.

3-2 منهجية الدراسة:

استخدمت هذه الدراسة المنهج الوصفي في عرض البيانات وتحليل نتائج الإستبانة التي تم توزيعها على عينة الدراسة.

3-3 مجتمع الدراسة وعينتها:

يتكون مجتمع الدراسة من المحاسبين والمدققين الداخليين وموظفي تكنولوجيا المعلومات بمختلف درجاتهم الوظيفية في الشركات الصناعية الأردنية والتي تقوم باستخدام نظم المعلومات المحاسبية في إدخال ومعالجة البيانات، وقد وتم اختيار عينة عشوائية من 30 شركة صناعية مساهمة عامة أو ذات مسؤولية محدودة عاملة في الأردن وتستخدم نظم المعلومات المحاسبية.

قام الباحث بتوزيع (145) استبانة على أفراد عينة الدراسة واسترداد (72) استبانة صالحة للتحليل وذلك بنسبة استرداد بلغت حوالي 50%، وراعى الباحث في اختياره لهذه الشركات عدة معايير وهي استخدامها لنظم المعلومات المحاسبية وأن تكون ضمن الشركات الصناعية العاملة في الأردن.

3-4 أداة الدراسة ومصادر الحصول على المعلومات:

3-4-1 مصادر الحصول على المعلومات:

تم الاعتماد على نوعين من المصادر للحصول على المعلومات اللازمة لهذه الدراسة وهما:

3-4-1-1 مصادر المعلومات الأولية:

تم الاستعانة بالاستبانة كأداة القياس الرئيسية والتي تم تصميمها لجمع البيانات والمعلومات اللازمة لهذه الدراسة، حيث تم توزيعها على أفراد عينة الدراسة بهدف التعرف على إجابات أفراد العينة حول مدى تأثير الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية، وقد قام الباحث بتوزيع الاستبانات على عينة الدراسة بشكل شخصي وعمل على اللقاء مع الشخص المعني بتوزيع الاستبانة في الشركات الصناعية الأردنية بهدف توضيح الغاية من هذه الدراسة وأن المعلومات التي يتم جمعها سوف تعامل بسرية تامة ولغايات البحث العلمي فقط، وقد تم جمع الاستبانات في وقت لاحق، حيث يتوقع من هذا الاسلوب أن يكون عدد المستجيبين أكبر مقارنة مع التوزيع البريدي أو الإلكتروني دون المساس بموثوقية النتائج إذ إن الباحث لا يتدخل في الإجابة. (Abdullatif & Kawuq, 2012)

3-4-1-2 مصادر المعلومات الثانوية:

تم تحديد الإطار النظري بالاعتماد على الكتب والمراجع والدوريات العلمية والتقارير والدراسات السابقة ذات الصلة بالموضوع.

3-4-2 أداة الدراسة:

لتحقيق أهداف الدراسة تم تصميم وتطوير استبانة مع الأخذ بعين الاعتبار الأدبيات والدراسات السابقة ذات الصلة بالموضوع وتكونت الاستبانة من الأجزاء التالية:

الجزء الأول : يخصص هذا الجزء من الاستبانة لجمع معلومات شخصية عن أفراد مجتمع الدراسة إذ احتوى على (العمر والدور الوظيفي والرتبة الوظيفية والمؤهل العلمي وسنوات الخبرة والشهادات المهنية.

الجزء الثاني : احتوى هذا الجزء على معلومات خاصة بالشركة (تصنيف الشركة وعدد موظفيها ونوع الشركة).

الجزء الثالث : احتوى هذا الجزء على 36 سؤالا تتعلق بالفرضية الأولى الخاصة بمدى فاعلية إجراءات الرقابة الداخلية في منع الاحتيال الإلكتروني المتعلق بأمن المعلومات قبل أن يحدث، وعلى 18 سؤالا خاصة بالفرضية الثانية وهي مدى فاعلية إجراءات الرقابة الداخلية في اكتشاف الاحتيال الإلكتروني المتعلق بأمن المعلومات بعد أن يحدث، وعلى 18 سؤالا تتعلق بالفرضية الثالثة وهي مدى فاعلية إجراءات الرقابة الداخلية في تصحيح ثغرات النظام التي تسببت بالاحتيال الإلكتروني المتعلق بأمن المعلومات.

الجزء الرابع : احتوى هذا الجزء على ستة أسئلة تتعلق بالفرضية الرابعة وهي بيان المعوقات التي قد تؤثر على فاعلية إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية.

وقد تم عرض الأسئلة المتعلقة بالفرضيات الأولى والثانية والثالثة على أساس عرض تسعة مخاطر مختلفة تنتمي إلى أمن معلومات نظم المعلومات المحاسبية الإلكترونية ولكل خطر يتم السؤال عن مدى أهميته من حيث نوع الاستجابات المحتملة في حال وجوده، إذ تم عرض ثمانية استجابات محتملة لكل خطر (ثم تم تكرارها لكل خطر بما يسمح بالمقارنة بين الإجابات) تمثل ثلاثة أنواع لإجراءات الرقابة الداخلية وهي كالتالي:

1- إجراءات تتعلق بالرقابة الوقائية وهي:

أ- التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.

ب-تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.

ج-تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.

د- استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.

2- إجراءات تتعلق بالرقابة الاكتشافية وهي:

أ- إنشاء سجل دخول للنظام.

ب-اختبار النظام والتدقيق عليه بشكل دوري.

3- إجراءات تتعلق بالرقابة التصحيحية وهي:

أ- وجود فريق استجابة للتهديدات التي تعرض لها النظام.

ب-تحديث البرمجيات المتخصصة بشكل دوري، ومن الأمثلة على ذلك تحديث مقاوم الفيروسات.

وقد تم اختيار المخاطر المختلفة من ثلاثة مجموعات رئيسية للمخاطر وهي مخاطر اختراق الشبكة (Hacking) ومخاطر الهندسة الاجتماعية (Social Engineering) ومخاطر البرمجيات الضارة (Malware) وذلك حسب التصنيف الوارد في Romney & Steinbart (2012)، فتم اختيار ثلاثة أخطار من كل مجموعة بهدف اختبار قدرة الأنظمة الرقابية في الشركات الصناعية الأردنية على منع واكتشاف وتصحيح الخلل لكل مجموعة من أنواع المخاطر الإلكترونية.

أما الفرضية الرابعة فقد تم عرض ستة أسئلة توضح المعوقات التي قد تواجهها الشركات لتفعيل اجراءات الرقابة الداخلية على أمن المعلومات وهي عدم الخضوع لتدريب مستمر حول أساليب الاحتيال الإلكتروني وعدم وعي مستخدمي النظام بأهمية الرقابة على تكنولوجيا المعلومات و عدم التزام مستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة و التطور المتسارع لأساليب الاحتيال الإلكتروني وعدم اهتمام ودعم الإدارة العليا لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات وارتفاع كلفة تنفيذ إجراءات الرقابة الداخلية على أمن المعلومات.

مقياس الاستبيان:

تم اعتماد مقياس (Likert Scale) المكون من خمس درجات لتحديد مدى فاعلية الإجراءات التي تقوم بها الشركات، حيث تتدرج الإجابات بين عدم توفر الإجراء أصلاً ممثلة بالقيمة (1) وتوفره مع فاعليته بشكل كبير ممثلة بالقيمة (5).

وللحكم على درجة الفاعلية لمتوسطات إجابات أسئلة الإستبانة الموضحة في جداول الفصل الرابع تم اختيار المقياس التالي والموضح بالجدول رقم (3-1):

جدول (3-1)

مقياس تحديد الأهمية النسبية للوسط الحسابي

الفترة	درجة الفعالية
2.99 – 1.00	منخفضة
3.99 – 3.00	متوسطة
4.49 – 4.00	مرتفعة
5.00 – 4.50	مرتفعة جدا

3-4-3 أداة الدراسة وموثوقيتها:

قام الباحث بتصميم الاستبانة بمساعدة المشرف وإرشاداته بالإضافة للاستعانة بمراجع ذات علاقة بموضوع البحث.

وتم التحقق من ثبات نتائج الاستبانة وموثوقيتها بتطبيق معامل كرونباخ ألفا (Cronbach Alpha) وكما هو موضح بالجدول رقم (3-2)، إذ يعتمد أسلوب كرونباخ ألفا على اتساق أداء الفرد من فقرة إلى أخرى والذي يشير إلى التماسك وقوة الارتباط بين فقرات المقياس. (Saunders, Lewis & Thornhill, 2012)

والجدول رقم (3-2) يوضح نتائج تطبيق اختبار كرونباخ ألفا على نتائج هذه الدراسة:

جدول (3-2)

معامل ثبات الاتساق الداخلي لمجالات الاستبانة (مقياس كرونباخ ألفا)

المجال	قيمة كرونباخ الفا	عدد الفقرات
إجراءات المنع	0.986	36
إجراءات الاكتشاف	0.972	18
إجراءات التصحيح	0.979	18
المعوقات	0.864	6
جميع الجُمل	0.991	78

تدل معاملات الثبات المبينة أعلاه في جدول رقم (3-2) على تمتع الأداة بصورة عامة بمعامل ثبات عال وبالتالي قدرة الأداة على تحقيق أغراض الدراسة، ويلاحظ أن جميع الأرقام أعلى من مستوى (70%) الذي يعد الحد الأدنى المقبول (Saunders, Lewis & Thornhill,

2012)، كما تدل على وجود تكرارات في أسئلة الاستبانة، إذ إن هذه التكرارات تعود إلى شكل تصميم الاستبانة من حيث تكرار مجموعة من الأسئلة لكل خطر إلكتروني، إذ إن هذا التكرار يؤدي إلى رفع قيمة معامل كرونباخ ألفا.

3-5 المعالجة الإحصائية المستخدمة:

للإجابة عن أسئلة الدراسة واختبار فرضياتها قام الباحث باستخدام الأساليب الإحصائية المناسبة في التحليل، والتي تعتمد على نوع البيانات المراد تحليلها، وعلى أهداف وفرضيات الدراسة وذلك من خلال استخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) وذلك لتحليل البيانات التي تم جمعها في هذه الدراسة وقد تم استخدام عدة أساليب إحصائية من أجل تحليل البيانات التي تم جمعها بشكل يؤدي إلى تحقيق أهداف الدراسة وفيما يلي الأساليب الإحصائية التي تم استخدامها:

1- المتوسطات الحسابية والانحرافات المعيارية كاستعراض لنتائج الدراسة بشكل مفصل وترتيب المخاطر حسب أهميتها.

2- تطبيق اختبار one sample t-test وذلك من أجل مقارنة الوسط الحسابي لمجموعة أسئلة الاستبانة مع المتوسط الفرضي لإجابات الاستبانة والبالغة قيمته (3) وهذا يُطبق للفرضيات الرئيسية الأولى والثانية والثالثة والرابعة.

3- بالنسبة للفرضية الخامسة فإنه تم استخدام اختبار (Mann - Whitney test) وذلك للمقارنات بين فئتين، واختبار (Kruskal - Wallis test) للمقارنة بين فئات يزيد عددها عن اثنتين.

الفصل الرابع

نتائج الدراسة واختبار الفرضيات

الفصل الرابع

نتائج الدراسة واختبار الفرضيات

4-1 المقدمة

4-2 وصف خصائص عينة الدراسة

4-3 استعراض نتائج الدراسة

4-4 اختبار فرضيات الدراسة

4-1 المقدمة:

يهدف هذا الفصل بشكل أساسي إلى عرض نتائج التحليل الإحصائي التي تم التوصل إليها، سوف يتم في هذا الفصل وصف أفراد عينة الدراسة وكذلك عرض لأسئلة الدراسة و من ثم اختبار فرضيات الدراسة.

4-2 وصف خصائص عينة الدراسة:

يتبين من تحليل النتائج المتعلقة بالجزء الأول من الاستبانة الخاصة بالمعلومات الشخصية والخصائص الديموغرافية لعينة الدراسة والموضحة بالجدول رقم (4-1) فيما يتعلق بالعمر فقد تم تقسيم هذا المتغير إلى فئات مختلفة الحجم بناءً على أن المستجيبين من الفئات الأصغر عمراً أكثر عدداً وذلك لأن الشركات الصناعية تحتوي على عدد أكبر بكثير من فئات الموظفين الأصغر عمراً وخبرة مقارنة بالأكثر عمراً وخبرة، كما أن عدم تساوي الفئات العمرية طولاً يعود أيضاً إلى أن الفرد في الفئات العمرية الأصغر أكثر احتمالاً لتغيير رأيه من الفرد في الفئات العمرية الأكبر .(الخطيب، 2012، ص 56)

والجدول التالي رقم (4-1) يوضح توزيع العينة حسب الخصائص الديموغرافية:

الجدول رقم (4-1)

توزيع العينة حسب الخصائص الديموغرافية

الرقم	المتغير	الفئة	التكرار	النسبة المئوية
1	العمر	أقل من 25 سنة	22	%30.6
		بين 25 و 30 سنة	27	%37.5
		بين 31 و 40 سنة	21	%29.2
		بين 41 و 50 سنة	2	%2.7
		أكثر من 50 سنة	0	%0
2	الدور الوظيفي	المحاسبة والإدارة المالية	29	%40.3
		التدقيق والرقابة الداخلية	12	%16.7
		تكنولوجيا المعلومات وأنظمة المعلومات الحاسوبية	31	%43.0
3	الرتبة الوظيفية	موظف مبتدئ	22	%30.6
		موظف رئيسي	30	%41.7
		مسؤول قسم	14	%19.4
		مدير دائرة	6	%8.3
4	المؤهل العلمي	دبلوم كلية مجتمع	3	%4.2
		بكالوريوس	56	%77.7
		دبلوم دراسات عليا	4	%5.6
		ماجستير	9	%12.5
		دكتوراه	0	%0

5	سنوات الخبرة	أقل من 5 سنوات	31	%43.1
		بين 5 و 10 سنوات	27	%37.4
		بين 11 و 15 سنة	11	%15.3
		بين 16 و 20 سنة	2	%2.8
		أكثر من 20 سنة	1	%1.4
6	الشهادات المهنية	نعم	24	%33.3
		لا	48	%66.7
7	تصنيف الشركة	شركة محلية	37	%51.4
		شركة أجنبية	35	%48.6
8	عدد الموظفين العاملين في الشركة	أقل من 50 موظف	5	%6.9
		من 50 إلى 100 موظف	5	%6.9
		أكثر من 100 موظف	62	%86.2
9	نوع الشركة	مساهمة عامة	26	%36.1
		ذات مسؤولية محدودة	46	%63.9

وتبين أن عدد المستجيبين من الفئة العمرية الأقل من 25 سنة 22 مستجيباً وبنسبة 30.6 % ، في حين بلغ عدد المستجيبين من الفئة العمرية بين 25 و 30 سنة 27 مستجيباً وبنسبة 37.5 % ، بينما بلغ عدد المستجيبين من الفئة العمرية بين 31 و 40 سنة 21 مستجيباً وبنسبة 29.2 % ، أما عدد المستجيبين من الفئة العمرية بين 41 و 50 سنة فقد بلغ مستجيبان فقط وبنسبة مئوية 2.7 % ، ولا يوجد أي مستجيب من الفئة العمرية أكبر من 50 سنة.

أما فيما يتعلق بالدور الوظيفي فلقد أظهرت النتائج أن عدد المستجيبين من فئة المحاسبة والإدارة المالية 29 مستجيباً وبنسبة 40.3 % ، أما من فئة التدقيق والرقابة الداخلية فلقد بلغ عدد المستجيبين 12 مستجيب وبنسبة مئوية 16.7 % ، أما من فئة تكنولوجيا المعلومات وأنظمة المعلومات الحاسوبية فقد بلغ عدد المستجيبين 31 مستجيباً وبنسبة 43 %.

أما فيما يتعلق بالرتبة الوظيفية فلقد أظهرت النتائج أن عدد المستجيبين من فئة موظف مبتدئ 22 مستجيباً وبنسبة 30.6 % ، أما من فئة موظف رئيسي فلقد بلغ عدد المستجيبين 30 مستجيباً وبنسبة مئوية 41.7 % ، أما من فئة مسؤول قسم 14 مستجيباً وبنسبة 19.4 % ، أما من فئة مدير دائرة ستة مستجيبين وبنسبة 8.3 %.

أما فيما يتعلق بالمؤهل العلمي فلقد أظهرت النتائج أن عدد المستجيبين من فئة دبلوم كلية مجتمع ثلاثة مستجيبين وبنسبة 4.2 % ، أما عدد المستجيبين من فئة بكالوريوس 56 مستجيباً وبنسبة 77.7 % ، أما من فئة دبلوم دراسات عليا أربعة مستجيبين وبنسبة 5.6 % ، أما من فئة ماجستير فلقد بلغ عدد المستجيبين تسعة مستجيبين وبنسبة مئوية 12.5 % ، ولا يوجد أي مستجيب من فئة الدكتوراه.

أما فيما يتعلق بسنوات الخبرة العملية في مجال عمل المستجيب فلقد بلغ عدد المستجيبين من فئة الأقل من خمس سنوات 31 مستجيباً وبنسبة 43.1 % ، أما من الفئة بين 5 و 10 سنوات 27 مستجيباً وبنسبة 37.4 % ، بينما بلغ عدد المستجيبين من الفئة بين 11 و 15 سنة 11 مستجيب وبنسبة 15.3 % ، أما من الفئة بين 16 و 20 سنة مستجيبين اثنين وبنسبة 2.8 % ، في حين بلغ عدد المستجيبين من الفئة أكثر من 20 سنة مستجيب واحد وبنسبة 1.4 %.

تظهر النتائج أن النسبة الأكبر لمن يمتلكون خبرة أقل من خمس سنوات وهذا متوقع لكثرة نسبة هؤلاء في الشركات الصناعية مقارنة بمن هم أكثر خبرة.

أما فيما يتعلق بالشهادات المهنية فلقد بلغ عدد المستجيبين من الفئة "نعم" 24 مستجيباً وبنسبة 33.3 % ، بينما بلغ عدد المستجيبين من الفئة "لا" 48 مستجيباً وبنسبة 66.7 % ، مما يظهر تفاوتاً كبيراً بين عدد من يحملون الشهادات المهنية وممن لا يحملونها.

تظهر النتائج أن نسبة مَن لا يحملون الشهادات المهنية أكبر بكثير من نسبة من يحملون الشهادات المهنية وقد يعود ذلك من وجهة نظر الباحث إلى أن الحصول على هذه الشهادات المهنية مكلف نسبيا وكذلك يحتاج إلى المزيد من الوقت والتفرغ.

أما فيما يتعلق بتصنيف العينة من حيث كونها شركة محلية أو أجنبية فلقد كان عدد المستجيبين من الفئة الشركات المحلية 37 مستجيباً وبنسبة 51.4 % ، أما من فئة الشركات الأجنبية 35 مستجيباً وبنسبة 48.6 %.

أما فيما يتعلق بعدد الموظفين في الشركة الصناعية فلقد بلغ عدد المستجيبين من الفئة الأقل من 50 موظف خمسة مستجيبين وبنسبة 6.9% ، و من الفئة من 50 إلى 100 موظف خمسة مستجيبين وبنسبة 6.9 % ، في حين بلغ عدد المستجيبين من الفئة الأكثر من 100 موظف 62 مستجيباً وبنسبة مئوية 86.2 %.

وتظهر النتائج أن أكبر نسبة استجابة كانت ضمن الشركات التي يعمل فيها أكثر من 100 موظف، ويرى الباحث أن هذه نقطة قوه في عينة الدراسة، وذلك بسبب احتوائها على عدد كبير من مستخدمي أجهزة الحاسوب.

أما فيما يتعلق بنوع الشركة الصناعية (شكلها القانوني) فلقد بلغ عدد المستجيبين من فئة الشركات المساهمة العامة 26 مستجيباً وبنسبة 36.1% ، أما من الفئة الشركات ذات المسؤولية المحدودة 46 مستجيباً وبنسبة 63.9%.

وبشكل عام يتضح من الجدول رقم (4-1) بأن أفراد عينة الدراسة تمتلك بشكل عام الخبرة والكفاءة اللازمتان للإجابة عن أسئلة الاستبانة بشكل معقول، وهم موزعون بشكل مناسب على أنواع الشركات والشهادات والدور الوظيفي وغير ذلك مما يدعم جودة الإجابات على الأسئلة.

4-3 استعراض نتائج الدراسة:

للتعرف على مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية من خلال تطبيق إجراءات الرقابة الداخلية المتعلقة بأمن المعلومات والتعرف على الاستجابات المطبقة في حالة وجود المخاطر المتعلقة بأمن المعلومات، فقد تم استخدام المتوسطات الحسابية والانحرافات المعيارية ومستوى الموافقة كما هو موضح في الجداول التالية:

4-3-1 مخاطر اختراق الشبكة (Hacking):

4-3-1/أ إجراءات الرقابة الداخلية على مخاطر سرقة كلمة السر (Password Cracking):

يبين جدول رقم (4-3-1/أ) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة على مخاطر سرقة كلمة السر.

الجدول رقم (4-3-1/أ)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
1	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.22	1.078	مرتفعة
2	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.75	0.783	مرتفعة جدا
3	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.68	0.728	مرتفعة جدا
4	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.49	1.088	مرتفعة
5	إنشاء سجل دخول للنظام.	4.49	1.035	مرتفعة
6	اختبار النظام والتدقيق عليه بشكل دوري.	4.39	1.015	مرتفعة
7	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	4.29	1.131	مرتفعة
8	تحديث البرمجيات المتخصصة بشكل دوري.	4.33	1.138	مرتفعة
	المتوسط الحسابي للمجموعة	4.46		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه فيما يتعلق بمخاطر سرقة كلمة السر حصول الفقرة " تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك " على المرتبة

الأولى وبمتوسط حسابي 4.75 وانحراف معياري 0.783 بينما حصلت الفقرة " التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة " على المرتبة الأخيرة وبمتوسط حسابي 4.22 وانحراف معياري 1.078.

ويلاحظ بأن درجة الموافقة على وجود الإجراءات المعنية وفاعليتها كان مرتفعاً جداً وبخاصة في مجال المنع بينما كان أقل في مجال الاكتشاف والتصحيح، وقد يعود ذلك لرأي الشركات الصناعية بأن التركيز على إجراءات المنع لهذا الخطر سيؤدي لتقليل الخسائر التي قد تتعرض لها الشركات، وعلى سبيل المثال فإن المبالغ التي يتم إنفاقها من قبل الشركات الصناعية للمحافظة على أمن معادلات التصنيع الخاصة بها أكثر فائدة من تلك التي يتم إنفاقها على الإجراءات اللازمة للكشف عن سرقتها.

4-3-1/ ب إجراءات الرقابة الداخلية على مخاطر التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack):

يبين جدول رقم (4-3-1/ب) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة في حالة التعرض للاختراق أثناء محاولة معالجة اختراق سابق:

الجدول رقم (4-3-1/ب)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
9	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.93	1.214	متوسطة
10	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.26	1.210	مرتفعة
11	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.28	1.201	مرتفعة
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.22	1.270	مرتفعة
13	إنشاء سجل دخول للنظام.	4.17	1.289	مرتفعة
14	اختبار النظام والتدقيق عليه بشكل دوري.	4.07	1.248	مرتفعة
15	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	4.04	1.283	مرتفعة
16	تحديث البرمجيات المتخصصة بشكل دوري.	4.21	1.221	مرتفعة
	المتوسط الحسابي للمجموعة	4.15		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة " تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم " على المرتبة الأولى وبمتوسط

حسابي 4.28 وانحراف معياري 1.201 بينما حصلت الفقرة " التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة " على المرتبة الأخيرة وبمتوسط حسابي 3.93 وانحراف معياري 1.214.

4-3-1/ ج إجراءات الرقابة الداخلية على مخاطر هجمات حقن قواعد البيانات (SQL Injection Attack):

يبين جدول رقم (4-3-1/ج) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة على مخاطر هجمات حقن قواعد البيانات:

الجدول رقم (4-3-1/ج)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
17	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.83	1.300	متوسطة
18	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.22	1.213	مرتفعة
19	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.26	1.175	مرتفعة
20	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.26	1.245	مرتفعة
21	إنشاء سجل دخول للنظام.	4.08	1.286	مرتفعة

22	اختبار النظام والتدقيق عليه بشكل دوري.	4.07	1.191	مرتفعة
23	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	4.14	1.190	مرتفعة
24	تحديث البرمجيات المتخصصة بشكل دوري.	4.18	1.179	مرتفعة
	المتوسط الحسابي للمجموعة	4.13		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة " تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم " والفقرة " استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة "على المرتبة الأولى وبمتوسط حسابي 4.26 لكليهما وانحراف معياري 1.175 و 1.245 على التوالي بينما حصلت الفقرة " التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة " على المرتبة الأخيرة وبمتوسط حسابي 3.83 وانحراف معياري 1.300.

ويلاحظ بأن درجة الموافقة على وجود الإجراءات المعنية وفاعليتها كان مرتفعاً ضمن إجراءات الرقابة الداخلية لمواجهة مخاطر التعرض للاختراق أثناء معالجة اختراق سابق وإجراءات الرقابة الداخلية على مخاطر هجمات حقن قواعد البيانات على الرغم من أن فاعلية التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة كانت متوسطة وقد يعود ذلك لرأي أفراد العينة من المحاسبين بأنهم غير معنيين بهذا الخطر كما هو موضح في الجدول رقم (4–4–6)، كما يلاحظ بأن فاعلية إجراءات الرقابة الداخلية في مواجهة مخاطر سرقة كلمة السر كانت أعلى منها لمخاطر التعرض لاختراق أثناء معالجة اختراق

سابق و مخاطر هجمات حقن قواعد البيانات، وقد يعود ذلك إلى معرفة عينة الدراسة لخطر سرقة كلمة السر أكثر من الخطرين الآخرين.

4-3-2 مخاطر الهندسة الاجتماعية (Social Engineering)

4-3-2/أ إجراءات الرقابة الداخلية على مخاطر إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin):

يبين جدول رقم (4-3-2/أ) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة الداخلية على مخاطر إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به:

الجدول رقم (4-3-2/أ)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
25	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.86	1.225	متوسطة
26	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.08	1.184	مرتفعة
27	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.14	1.179	مرتفعة
28	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.13	1.221	مرتفعة
29	إنشاء سجل دخول للنظام.	4.14	1.271	مرتفعة
30	اختبار النظام والتدقيق عليه بشكل دوري.	4.15	1.057	مرتفعة
31	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	4.13	1.138	مرتفعة
32	تحديث البرمجيات المتخصصة بشكل دوري.	4.25	1.097	مرتفعة
	المتوسط الحسابي للمجموعة	4.11		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة " تحديث البرمجيات المتخصصة بشكل دوري " على المرتبة الأولى وبمتوسط حسابي 4.25 وانحراف معياري 1.097

بينما حصلت الفقرة " التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة " على المرتبة الأخيرة وبمتوسط حسابي 3.86 وانحراف معياري 1.225 .

4-3-2/ ب إجراءات الرقابة الداخلية على مخاطر إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft):

يبين جدول رقم (4-3-2/ب) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة الداخلية على مخاطر إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر:

الجدول رقم (4-3-2/ب)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
33	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.97	1.210	متوسطة
34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.14	1.214	مرتفعة
35	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.11	1.306	مرتفعة
36	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.18	1.248	مرتفعة
37	إنشاء سجل دخول للنظام.	3.99	1.409	متوسطة
38	اختبار النظام والتدقيق عليه بشكل دوري.	4.07	1.237	مرتفعة
39	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	3.94	1.277	متوسطة
40	تحديث البرمجيات المتخصصة بشكل دوري.	4.06	1.277	مرتفعة
	المتوسط الحسابي للمجموعة	4.06		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة " استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة " على المرتبة الأولى وبمتوسط

حسابي 4.18 وانحراف معياري 1.248 بينما حصلت الفقرة " وجود فريق استجابة للتهديدات التي تعرض لها النظام " على المرتبة الأخيرة وبمتوسط حسابي 3.94 وانحراف معياري 1.277.

4-3-2/ ج إجراءات الرقابة الداخلية على مخاطر وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة (Phishing):

يبين جدول رقم (4-3-2/ج) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة الداخلية على مخاطر وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة:

الجدول رقم (4-3-2/ج)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
41	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.01	1.284	مرتفعة
42	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.18	1.167	مرتفعة
43	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.11	1.295	مرتفعة

44	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	3.92	1.340	متوسطة
45	إنشاء سجل دخول للنظام.	4.03	1.404	مرتفعة
46	اختبار النظام والتدقيق عليه بشكل دوري.	4.14	1.225	مرتفعة
47	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	4.08	1.253	مرتفعة
48	تحديث البرمجيات المتخصصة بشكل دوري.	4.08	1.275	مرتفعة
	المتوسط الحسابي للمجموعة	4.07		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة "تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك " على المرتبة الأولى وبمتوسط حسابي 4.18 وانحراف معياري 1.167 بينما حصلت الفقرة " استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة " على المرتبة الأخيرة وبمتوسط حسابي 3.92 وانحراف معياري 1.340.

ويلاحظ بأن درجة الموافقة على وجود الإجراءات المعنية وفاعليتها لمواجهة مخاطر الهندسة الاجتماعية كانت مرتفعة ومتقاربة في جميع المجالات (المنع والاكتشاف والتصحيح) على الرغم من أن فقرة التوعية والتدريب كانت متوسطة أو مرتفعة بشكل نسبي، وقد يعود هذا الارتفاع النسبي لانتشار مخاطر الهندسة الاجتماعية في الآونة الأخيرة وبالتالي أصبحت مألوفة من قبل مستخدمي أجهزة الحاسوب.

3-3-4 مخاطر البرمجيات الضارة (Malware):

4-3-3/ أ إجراءات الرقابة الداخلية على مخاطر البرامج التي تظهر بأنها تعمل بشكل معين ومفيد للمستخدم بينما هي في الواقع تقوم بعمل ضار وخفي عن المستخدم (Trojan Horse):

يبين جدول رقم (4-3-3/أ) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة الداخلية على مخاطر البرامج التي تظهر بأنها تعمل بشكل معين ومفيد للمستخدم بينما هي في الواقع تقوم بعمل ضار وخفي عن المستخدم:

الجدول رقم (4-3-3/أ)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
49	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.97	1.353	متوسطة
50	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.06	1.255	مرتفعة
51	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.21	1.266	مرتفعة
52	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.24	1.305	مرتفعة

53	إنشاء سجل دخول للنظام.	4.15	1.329	مرتفعة
54	اختبار النظام والتدقيق عليه بشكل دوري.	4.15	1.229	مرتفعة
55	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	4.13	1.278	مرتفعة
56	تحديث البرمجيات المتخصصة بشكل دوري.	4.18	1.325	مرتفعة
	المتوسط الحسابي للمجموعة	4.14		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة " استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة " على المرتبة الأولى وبمتوسط حسابي 4.24 وانحراف معياري 1.305 بينما حصلت الفقرة " التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة " على المرتبة الأخيرة وبمتوسط حسابي 3.97 وانحراف معياري 1.353.

ويلاحظ بأن درجة الموافقة على وجود الإجراءات المعنية وفاعليتها كان متقارباً بين جميع المجالات، وقد يعود ذلك بسبب توسع الشركات الصناعية في استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة بالإضافة لفرض رقابة شديدة من شأنها تقييد تنزيل الملفات من خلال الإنترنت.

4-3-3/ ب إجراءات الرقابة الداخلية على مخاطر الفيروسات (Viruses):

يبين جدول رقم (4-3-3/ب) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة الداخلية على مخاطر الفيروسات:

الجدول رقم (4-3-3/ب)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
57	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.26	1.113	مرتفعة
58	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.35	1.023	مرتفعة
59	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.47	1.048	مرتفعة
60	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.40	1.134	مرتفعة
61	إنشاء سجل دخول للنظام.	4.26	1.175	مرتفعة
62	اختبار النظام والتدقيق عليه بشكل دوري.	4.35	1.050	مرتفعة
63	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	4.32	1.136	مرتفعة
64	تحديث البرمجيات المتخصصة بشكل دوري.	4.43	1.124	مرتفعة
	المتوسط الحسابي للمجموعة	4.36		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة " تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم " على المرتبة الأولى وبمتوسط حسابي 4.47 وانحراف معياري 1.048 بينما حصلت الفقرتين " التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة " وبمتوسط حسابي 4.26 وانحراف معياري 1.113 والفقرة "إنشاء سجل دخول للنظام" وبمتوسط حسابي 4.26 وانحراف معياري 1.175 على المرتبة الأخيرة.

ويلاحظ بأن درجة الموافقة على وجود الإجراءات المعنية وفاعليتها كان مرتفعاً بشكل ملحوظ ومتقارباً بين جميع المجالات، وقد يعود ذلك كون هذه التقنية مألوفة بشكل كبير جداً من قبل مستخدمي الحاسوب.

4-3-3/ ج إجراءات الرقابة الداخلية على مخاطر البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware):

يبين جدول رقم (4-3-3/ج) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بالرقابة الداخلية على مخاطر البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت:

الجدول رقم (4-3-3/ج)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
65	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.89	1.400	متوسطة
66	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.07	1.293	مرتفعة
67	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.14	1.271	مرتفعة
68	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	4.06	1.362	مرتفعة
69	إنشاء سجل دخول للنظام.	4.01	1.389	مرتفعة
70	اختبار النظام والتدقيق عليه بشكل دوري.	3.89	1.327	متوسطة
71	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	3.89	1.430	متوسطة
72	تحديث البرمجيات المتخصصة بشكل دوري.	4.07	1.357	مرتفعة
	المتوسط الحسابي للمجموعة	4.00		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة "تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم " على المرتبة الأولى وبمتوسط حسابي

4.14 وانحراف معياري 1.271 والفقرات " التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة " وبمتوسط حسابي 3.89 وانحراف معياري 1.400 و" اختبار النظام والتدقيق عليه بشكل دوري " وبمتوسط حسابي 3.89 وانحراف معياري 1.327 و " وجود فريق استجابة للتهديدات التي تعرض لها النظام " وبمتوسط حسابي 3.89 وانحراف معياري 1.430 على المرتبة الأخيرة.

4-3-4 أنواع إجراءات الرقابة الداخلية:

يبين جدول رقم (4-3-4) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على إجراءات الرقابة الداخلية على أمن المعلومات:

جدول رقم (4-3-4)

الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
إجراءات الرقابة الداخلية الخاصة بالمنع	4.18	0.988	مرتفعة
إجراءات الرقابة الداخلية الخاصة بالإكتشاف	4.14	1.017	مرتفعة
إجراءات الرقابة الداخلية الخاصة بالتصحيح	4.15	1.054	مرتفعة
المتوسط الحسابي للمجموعة	4.16		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول رقم (4-3-4) تقارباً في استجابات أفراد العينة والمتمثل في الوسط الحسابي للمستجيبين بين إجراءات الرقابة الداخلية الثلاثة موضوع الدراسة،

ويرى الباحث بأن هذا متوقع إذ إن التطور المتسارع في أساليب الاحتيال الإلكتروني يفرض على الشركات الاهتمام بإجراءات الرقابة الداخلية الثلاثة موضوع الدراسة مع التركيز على إجراءات المنع لضمان تأكيد معقول بأن بياناتها محمية.

4-3-5 معوقات إجراءات الرقابة الداخلية على أمن المعلومات:

يبين جدول رقم (4-3-5) المتوسط الحسابي والانحراف المعياري لإجابات أفراد العينة على الإجراءات المتعلقة بمعوقات إجراءات الرقابة الداخلية على أمن المعلومات:

الجدول رقم (4-3-5)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الأهمية
73	عدم الخضوع لتدريب مستمر حول أساليب الاحتيال الإلكتروني.	4.13	1.020	مرتفعة
74	عدم وعي مستخدمي النظام بأهمية الرقابة على تكنولوجيا المعلومات	4.08	1.160	مرتفعة
75	عدم التزام مستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.01	1.169	مرتفعة
76	التطور المتسارع لأساليب الاحتيال الإلكتروني.	4.24	1.014	مرتفعة
77	عدم اهتمام ودعم الإدارة العليا لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات.	4.17	1.048	مرتفعة
78	ارتفاع كلفة تنفيذ إجراءات الرقابة الداخلية على أمن المعلومات.	3.86	1.066	متوسطة
	المتوسط الحسابي للمجموعة	4.08		مرتفعة

لقد أظهرت النتائج الموضحة في الجدول أعلاه حصول الفقرة " التطور المتسارع لأساليب الاحتيال الإلكتروني " على المرتبة الأولى وبمتوسط حسابي 4.24 وانحراف معياري 1.014 بينما حصلت الفقرة " ارتفاع كلفة تنفيذ إجراءات الرقابة الداخلية على أمن المعلومات " على المرتبة الأخيرة وبمتوسط حسابي 3.86 وانحراف معياري 1.066.

ويلاحظ بأن درجة الموافقة على وجود تأثير المعوقات أعلاه على فاعلية إجراءات الرقابة الداخلية مرتفعة باستثناء معوق الكلفة فقد كانت متوسطة، وقد يعود ذلك لأهمية تنفيذ إجراءات الرقابة الداخلية للمحافظة على أمن المعلومات مع الأخذ بعين الاعتبار الموازنة بين كلفة هذه الإجراءات ومنفعتها.

وإن درجة الموافقة المرتفعة على وجود المعوقات المذكورة في الجدول رقم (4-3-5) تستدعي المزيد من الانتباه لدى الشركات الصناعية الأردنية فيما يتعلق بتطوير نظم المعلومات المحاسبية لديها جنباً الى جنب مع تطوير الإجراءات اللازمة للرقابة على أمن المعلومات الالكترونية لديها.

4-4 اختبار فرضيات الدراسة:

قام الباحث بعمل اختبار لفرضيات الدراسة الرئيسية والفرعية من خلال استخدام اختبار (One Sample t-test) لاختبار مدى قبول أو رفض فرضيات الدراسة حيث أنه ترفض الفرضية العدمية إذا كانت قيم (t) المحسوبة أكبر من قيمتها الجدولية، أو إذا كانت الدلالة ≤ 0.05، وذلك كما يلي:

الفرضية الرئيسية الأولى H01 لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني المرتبط بأمن المعلومات قبل حدوثه، ويتفرع عن هذه الفرضية الفرضيات الفرعية التالية:

1- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني الخاص باختراق الشبكات الحاسوبية (Hacking) قبل حدوثه.

2- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني الخاص بالهندسة الاجتماعية (Social Engineering) قبل حدوثه.

3- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في منع الاحتيال الإلكتروني الخاص بالبرمجيات الضارة (Malware) قبل حدوثه.

لاختبار هذه الفرضيات تم استخدام اختبار **(**One Sample t-test**)** للتحقق من مدى ملاءمة استجابات الشركات الصناعية الأردنية لمخاطر لاحتيال الإلكتروني المرتبط بأمن المعلومات قبل حدوثه إذ أنه تم احتساب المتوسط الحسابي لكل استجابة على حده ومقارنتها مع الوسط الافتراضي للإجابات وهو (3)، كما هو موضح بالجدول (4-4-1)، وقد تم احتساب (t) الجدولية بناء على درجة الحرية (حجم العينة ناقص واحد). (Lind, Marchal & Wathen, 2010)

جدول رقم (4-4-1)

البيان	المتوسط الحسابي	الانحراف المعياري	T المحسوبة	T الجدولية	Sig* مستوى الدلالة	نتيجة اختبار الفرضية العدمية
منع مخاطر اختراق الشبكات الحاسوبية	4.285	0.965	11.300	1.994	0.000	رفض
منع مخاطر الهندسة الاجتماعية	4.069	1.065	8.519	1.994	0.000	رفض
منع مخاطر البرمجيات الضارة	4.176	1.066	9.361	1.994	0.000	رفض

* دالة إحصائيا عند مستوى (0.05) ≥ α

بناء على النتائج في الجدول رقم (4-4-1) فإن الفرضية العدمية الرئيسية الأولى ترفض وهذا معناه أن إجراءات الرقابة الداخلية الخاصة بمنع مخاطر أمن المعلومات فعالة في مواجهة مخاطر اختراق الشبكات الحاسوبية (Hacking) والهندسة الاجتماعية (Social Engineering) والبرمجيات الضارة (Malware).

وقد بلغت قيمة (t) المحسوبة للفرضية الفرعية الأولى وهي " منع مخاطر اختراق الشبكات الحاسوبية" (11.300) والفرضية الفرعية الثانية وهي " منع مخاطر الهندسة الاجتماعية " (8.519) أما الفرضية الفرعية الثالثة وهي " منع مخاطر البرمجيات الضارة " فقد بلغت قيمة (t) المحسوبة (9.361)، ويتضح أن قيم (t) المحسوبة في الحالات الثلاث كانت أكبر من الجدولية (1.994) كما أن الدلالة Sig (0.000) وهي دالة إحصائيا عند مستوى (α ≤ 0.05) بالمقارنة مع قيمة (t) الجدولية البالغة (1.994) وبناءً على ذلك **ترفض الفرضيات الفرعية العدمية.**

الفرضية الرئيسية الثانية H02 لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في كشف الاحتيال الإلكتروني المرتبط بأمن المعلومات بعد حدوثه، ويتفرع عن هذه الفرضية الفرضيات الفرعية التالية:

1- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في كشف الاحتيال الإلكتروني من خلال اختراق الشبكات (Hacking) والمرتبط بأمن المعلومات بعد حدوثه.

2- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في كشف الاحتيال الإلكتروني من خلال الهندسة الاجتماعية (Social Engineering) والمرتبط بأمن المعلومات بعد حدوثه.

3- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في كشف الاحتيال الإلكتروني من خلال البرمجيات الضارة (Malware) والمرتبط بأمن المعلومات بعد حدوثه.

لاختبار هذه الفرضيات تم استخدام اختبار **(**One Sample t-test**)** للتحقق من مدى ملاءمة استجابات الشركات الصناعية الأردنية لاكتشاف الاحتيال الإلكتروني المرتبط بأمن المعلومات بعد حدوثه إذ أنه تم احتساب المتوسط الحسابي لكل استجابة على حده ومقارنتها مع الوسط الافتراضي للإجابات وهو (3)، كما هو موضح بالجدول (4-4-2)، وقد تم احتساب (t) الجدولية بناء على درجة الحرية (حجم العينة ناقص واحد). (Lind, Marchal & Wathen, 2010)

جدول رقم (4-4-2)

البيان	المتوسط الحسابي	الانحراف المعياري	T المحسوبة	T الجدولية	Sig* مستوى الدلالة	نتيجة اختبار الفرضية العدمية
اكتشاف اختراق الشبكات الحاسوبية	4.211	1.013	10.139	1.994	0.000	رفض
اكتشاف الهندسة الاجتماعية	4.086	1.113	8.275	1.994	0.000	رفض
اكتشاف البرمجيات الضارة	4.137	1.096	8.802	1.994	0.000	رفض

* دالة إحصائيا عند مستوى (0.05) ≥ α

بناء على النتائج في الجدول رقم (4-4-2) فإن الفرضية العدمية الرئيسية الثانية ترفض وهذا معناه أن إجراءات الرقابة الداخلية الخاصة باكتشاف مخاطر أمن المعلومات فعالة في مواجهة مخاطر اختراق الشبكات الحاسوبية (Hacking) والهندسة الاجتماعية (Social Engineering) والبرمجيات الضارة (Malware).

وقد بلغت قيمة (t) المحسوبة للفرضية الفرعية الأولى وهي " اكتشاف اختراق الشبكات الحاسوبية" (10.139) والفرضية الفرعية الثانية وهي " اكتشاف الهندسة الاجتماعية " (8.275) أما الفرضية الفرعية الثالثة وهي " اكتشاف البرمجيات الضارة " فقد بلغت قيمة (t) المحسوبة (8.802)، ويتضح أن قيم (t) المحسوبة في الحالات الثلاث كانت أكبر من الجدولية (1.994) كما أن الدلالة Sig (0.000) وهي دالة إحصائيا عند مستوى (0.05 ≥ α) بالمقارنة مع قيمة (t) الجدولية البالغة (1.994) وبناءً على ذلك **ترفض الفرضيات الفرعية العدمية.**

الفرضية الرئيسية الثالثة H03 لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات، ويتفرع عن هذه الفرضية الفرضيات الفرعية التالية:

1- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات عن طريق اختراق الشبكات الحاسوبية (Hacking).

2- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات عن طريق الهندسة الاجتماعية (Social Engineering).

3- لا تتسم إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية بالفاعلية في تصحيح الثغرات التي تسببت بالاحتيال الإلكتروني المرتبط بأمن المعلومات عن طريق البرمجيات الضارة (Malware).

لاختبار هذه الفرضيات تم استخدام اختبار **(One Sample t-test)** للتحقق من مدى ملاءمة استجابات الشركات الصناعية الأردنية لتصحيح الثغرات التي أدت للاحتيال الإلكتروني المرتبط بأمن المعلومات، إذ أنه تم احتساب المتوسط الحسابي لكل استجابة على حده ومقارنتها مع الوسط الافتراضي للإجابات وهو (3) ، كما هو موضح بالجدول (4-4-3)، وقد تم احتساب (t) الجدولية بناء على درجة الحرية (حجم العينة ناقص واحد). (Lind, Marchal & Wathen, 2010)

جدول رقم (4-4-3)

البيان	المتوسط الحسابي	الانحراف المعياري	T المحسوبة	T الجدولية	Sig* مستوى الدلالة	نتيجة اختبار الفرضية العدمية
تصحيح الثغرات التي أدت الى إختراق الشبكات الحاسوبية	4.199	1.071	9.494	1.994	0.000	رفض
تصحيح الثغرات لمواجهة تهديدات الهندسة الإجتماعية	4.090	1.082	8.548	1.994	0.000	رفض
تصحيح الثغرات لمواجهة تهديدات البرمجيات الضارة	4.169	1.145	8.660	1.994	0.000	رفض

* دالة إحصائيا عند مستوى (0.05) ≥ α

بناء على النتائج في الجدول رقم (4-4-3) فإن الفرضية العدمية الرئيسية الثالثة ترفض وهذا معناه أن إجراءات الرقابة الداخلية الخاصة بتصحيح الثغرات التي تسببت بالاحتيال الالكتروني المرتبط بأمن المعلومات فعالة في مواجهة مخاطر اختراق الشبكات الحاسوبية (Hacking) والهندسة الاجتماعية (Social Engineering) والبرمجيات الضارة (Malware).

وقد بلغت قيمة (t) المحسوبة للفرضية الفرعية الأولى وهي " تصحيح الثغرات التي أدت الى اختراق الشبكات الحاسوبية " (9.494) والفرضية الفرعية الثانية وهي " تصحيح الثغرات لمواجهة تهديدات الهندسة الاجتماعية " (8.548) أما الفرضية الفرعية الثالثة وهي " تصحيح الثغرات لمواجهة تهديدات البرمجيات الضارة " فقد بلغت قيمة (t) المحسوبة (8.660)، ويتضح أن قيم (t) المحسوبة في الحالات الثلاث كانت أكبر من الجدولية (1.994) كما أن الدلالة Sig

(0.000) وهي دالة إحصائيا عند مستوى ($\alpha \leq 0.05$) بالمقارنة مع قيمة (t) الجدولية البالغة (1.994) وبناءً على ذلك **ترفض الفرضيات الفرعية العدمية.**

الفرضية الرئيسية الرابعة H04 لا توجد معوقات تؤثر على فاعلية إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية في الشركات الصناعية الأردنية.

لاختبار هذه الفرضية تم استخدام اختبار **(**One Sample t-test**)** للتحقق من مدى ملاءمة استجابات الشركات الصناعية الأردن للمعوقات التي تؤثر على تفعيل إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية، إذ أنه تم احتساب المتوسط الحسابي لكل استجابة على حده ومقارنتها مع الوسط الافتراضي للإجابات وهو (3)، كما هو موضح بالجدول (4-4-4)، وقد تم احتساب (t) الجدولية بناء على درجة الحرية (حجم العينة ناقص واحد). (Lind, Marchal & Wathen, 2010)

جدول رقم (4-4-4)

البيان	المتوسط الحسابي	الانحراف المعياري	T المحسوبة	T الجدولية	Sig* مستوى الدلالة	نتيجة اختبار الفرضية العدمية
معوقات تطبيق إجراءات الرقابة الداخلية	4.081	0.834	10.998	1.994	0.000	رفض

* دالة إحصائيا عند مستوى ($\alpha \leq 0.05$)

بناء على النتائج في الجدول رقم (4-4-4) فإن الفرضية العدمية الرئيسية الرابعة ترفض وهذا معناه وجود معوقات تؤثر على تفعيل إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية.

وقد أظهرت نتائج التحليل الاحصائي أنه توجد معوقات تؤثر على تفعيل إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية في الشركات الصناعية الأردنية، إذ بلغت قيمة (t) المحسوبة للفرضية وهي " معوقات تطبيق إجراءات الرقابة الداخلية " (10.998)، ويتضح أن قيمة (t) المحسوبة في الحالات السابقة كانت أكبر من الجدولية (1.994) كما أن الدلالة Sig (0.000) أقل من (0.05) وهي دالة إحصائيا عند مستوى ($\alpha \leq 0.05$) بالمقارنة مع قيمة (t) الجدولية البالغة (1.994) وبناءً على ذلك **ترفض الفرضية العدمية.**

الفرضية الرئيسية الخامسة H05 لا يوجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم، ويتفرع من هذه الفرضية الفرضيات الفرعية التالية:

1- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للعمر.

2- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للدور الوظيفي الحالي.

3- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للرتبة الوظيفية.

4- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للمؤهل العلمي.

5- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد سنوات الخبرة.

6- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للحصول على شهادات مهنية.

7- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لتصنيف الشركة.

8- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد الموظفين في الشركة.

9- لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لنوع الشركة.

الفرضية الفرعية الأولى :لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للعمر.

لاختبار هذه الفرضيات تم استخدام اختبار (Kruskal - Wallis test) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للعمر، وقد عمل الباحث على دمج فئة العمر بين إحدى وثلاثين وأربعين سنة و إحدى وأربعين وخمسين سنة مع فئة أكثر من خمسين سنة إذ إن أفراد عينة الدراسة في العمر أكثر من أربعين سنة قليلون

نسبياً وكما هو موضح بالجدول رقم (4-4-5)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير العمر وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-5)

المتغير: عمر أفراد العينة					
رقم الفقرة	الفقرة	أقل من 25 سنة	بين 25 و 30 سنة	أكثر من 30 سنة	P-Value
التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack)					
9	التوعية والتدريب المستمر لمستخدمي النظام.	3.45	3.96	4.35	0.031
16	تحديث البرمجيات المتخصصة بشكل دوري.	3.82	4.22	4.57	0.029
إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin).					
32	تحديث البرمجيات المتخصصة بشكل دوري.	3.86	4.30	4.57	0.043
إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft).					

36	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة.	3.73	4.44	4.30	0.042
40	تحديث البرمجيات المتخصصة بشكل دوري.	3.50	4.22	4.39	0.022
وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة (Phishing)					
48	تحديث البرمجيات المتخصصة بشكل دوري.	3.59	4.26	4.35	0.030
حصان طروادة (Trojan Horse): وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال.					
56	تحديث البرمجيات المتخصصة بشكل دوري.	3.55	4.44	4.48	0.023
البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware)					
72	تحديث البرمجيات المتخصصة بشكل دوري.	3.68	4.19	4.30	0.049

بالإشارة للجدول رقم (4-4-5) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا بين أفراد العينة تعود إلى العمر، ويلاحظ من الجدول السابق بأن ثمانية فقرات فقط أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة أي أن الغالبية العظمى لم ينتج عنها فروق إحصائية مهمة تعود إلى العمر، ويلاحظ أن المتوسطات الحسابية لاستجابات الفئة العمرية (أقل من 25 سنة) أقل من متوسط الاستجابات للفئات العمرية الأكبر، وعليه **لا ترفض الفرضية العدمية** أي أنه لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للعمر.

الفرضية الفرعية الثانية :لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للدور الوظيفي الحالي.

لاختبار هذه الفرضيات تم استخدام اختبار (Kruskal - Wallis test) وذلك من أجل التحقق من الفروق في إجابات أفراد عينة الدراسة تبعا للدور الوظيفي الحالي، كما هو موضح بالجدول رقم (4-4-6)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير الدور الوظيفي الحالي وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-6)

المتغير: الدور الوظيفي الحالي					
رقم الفقرة	الفقرة	المحاسبة والإدارة المالية	التدقيق والرقابة الداخلية	تكنولوجيا وأنظمة المعلومات الحاسوبية	P-Value
اختراق الشبكة والإطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة (Password cracking)					
4	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	4.07	4.83	4.74	0.036
8	تحديث البرمجيات المتخصصة بشكل دوري	3.86	4.66	4.65	0.002
التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack)					
9	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.45	4.50	4.16	0.024
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.72	4.75	4.48	0.037
13	إنشاء سجل دخول نظام المعلومات المحاسبي والشبكة الحاسوبية	3.69	4.83	4.35	0.017

15	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.55	4.67	4.26	0.024
16	تحديث البرمجيات المتخصصة بشكل دوري	3.55	4.67	4.65	0.000
هجمات حقن قواعد البيانات (SQL Injection Attack)					
17	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.52	4.58	3.84	0.048
18	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.79	4.83	4.39	0.019
20	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.83	4.75	4.48	0.024
21	إنشاء سجل دخول نظام المعلومات المحاسبي والشبكة الحاسوبية	3.62	4.83	4.23	0.012
22	اختبار نظام المعلومات المحاسبي والشبكة الحاسوبية والتدقيق عليهما بشكل دوري.	3.69	4.50	4.26	0.048
23	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.69	4.75	4.32	0.013
24	تحديث البرمجيات المتخصصة بشكل دوري	3.72	4.58	4.45	0.006

إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin)					
29	إنشاء سجل دخول نظام المعلومات المحاسبي والشبكة الحاسوبية	3.62	4.75	4.39	0.038
إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft)					
34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.62	4.33	4.55	0.016
35	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	3.41	4.42	4.65	0.003
36	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.62	4.67	4.52	0.002
37	إنشاء سجل دخول نظام المعلومات المحاسبي والشبكة الحاسوبية	3.31	4.67	4.35	0.008
39	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.34	4.58	4.26	0.005
40	تحديث البرمجيات المتخصصة بشكل دوري	3.48	4.50	4.42	0.004
وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة (Phishing)					

41	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.48	4.33	4.39	0.031
42	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.83	4.67	4.32	0.016
47	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.66	4.50	4.32	0.049
48	تحديث البرمجيات المتخصصة بشكل دوري	3.52	4.58	4.42	0.002
حصان طروادة (Trojan Horse): وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال					
49	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.38	4.58	4.29	0.038
50	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.52	4.75	4.29	0.009
52	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.59	4.83	4.61	0.003
55	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.62	4.75	4.35	0.028

56	تحديث البرمجيات المتخصصة بشكل دوري	3.52	4.75	4.58	0.001
الفيروسات (Viruses)					
58	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.00	4.83	4.48	0.026
60	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	4.03	4.92	4.55	0.039
63	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.97	4.83	4.45	0.036
64	تحديث البرمجيات المتخصصة بشكل دوري	4.00	4.83	4.68	0.004
البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware)					
65	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.34	4.17	4.29	0.046
66	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.59	4.50	4.35	0.024

71	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.31	4.33	4.26	0.012
72	تحديث البرمجيات المتخصصة بشكل دوري	3.55	4.58	4.35	0.004

بالإشارة للجدول رقم (4-4-6) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا بين أفراد العينة تعود إلى الدور الوظيفي، ويلاحظ من الجدول السابق بأن هناك 38 فقرة أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة وتتركز هذه الإجابات في 18 فقرة تتعلق بإجراءات الرقابة الداخلية الخاصة بمنع الخطر و15 فقرة تتعلق بإجراءات الرقابة الداخلية الخاصة بتصحيح الخطر وخمسة فقرات تتعلق بإجراءات الرقابة الداخلية الخاصة باكتشاف الخطر، ويلاحظ أيضاً وجود اتفاق بين أفراد العينة من المدققين الداخليين وموظفي قسم تكنولوجيا وأنظمة المعلومات الحاسوبية على فاعلية إجراءات الرقابة الداخلية بشكل مرتفع بينما يعود سبب الفروق في الاستجابات لتعارضها مع موظفي قسم المحاسبة والإدارة المالية، وقد يعود ذلك لاعتماد فئة المحاسبين والإدارة المالية على المدققين الداخليين وموظفي قسم تكنولوجيا المعلومات في مواجهة الأخطار الإلكترونية واعتقادهم بأنهم غير معنيين بهذه الأخطار أو عدم إدراكهم لإجراءات الرقابة الداخلية المتبعة في الشركة، وعليه **ترفض الفرضية العدمية** أي أنه توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للدور الوظيفي الحالي.

الفرضية الفرعية الثالثة :لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للرتبة الوظيفية.

لاختبار هذه الفرضيات تم استخدام اختبار (Kruskal - Wallis test) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للرتبة الوظيفية، وقد عمل الباحث على دمج فئة الرتبة الوظيفية مسؤول قسم وبين مدير دائرة إذ إن أفراد عينة الدراسة في الرتبة الوظيفية مدير دائرة قليلون نسبياً وكما هو موضح بالجدول رقم (4-4-7)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير الرتبة الوظيفية وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-7)

المتغير: الرتبة الوظيفية					
رقم الفقرة	الفقرة	موظف مبتدئ	موظف رئيسي	مسؤول قسم فأعلى	P-Value
إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin).					
25	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.23	4.27	3.95	0.017

32	تحديث البرمجيات المتخصصة بشكل دوري	3.91	4.27	4.60	0.044
إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft)					
34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	3.59	4.50	4.20	0.025
40	تحديث البرمجيات المتخصصة بشكل دوري	3.50	4.37	4.20	0.045
حصان طروادة (Trojan Horse): وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال					
51	تحديد صلاحيات مستخدمين النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم	3.59	4.63	4.25	0.010
53	إنشاء سجل دخول للنظام	3.64	4.53	4.15	0.046
الفيروسات (Viruses)					
64	تحديث البرمجيات المتخصصة بشكل دوري	4.05	4.70	4.45	0.023
البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware)					
69	إنشاء سجل دخول للنظام	3.55	4.37	4.00	0.037
72	تحديث البرمجيات المتخصصة بشكل دوري	3.55	4.27	4.35	0.016

بالإشارة للجدول رقم (4-4-7) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا بين أفراد العينة تعود إلى الرتبة الوظيفية، ويلاحظ من الجدول السابق بأنه فقط تسعة فقرات أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة أي أن الغالبية العظمى لم ينتج عنها فروق إحصائية مهمة تعود إلى الرتبة الوظيفية ويلاحظ أن المتوسطات الحسابية في الجدول موزعة بشكل شبه عشوائي، وأن أغلب الفروق كانت في الاستجابات المطبقة في "تحديث البرمجيات المتخصصة بشكل دوري" وقد يعود ذلك لكون الموظفين في المستويات الأعلى أكثر معرفة بمنافع تحديث البرمجيات بشكل دوري، وعليه **لا ترفض الفرضية العدمية** أي أنه لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للرتبة الوظيفية.

الفرضية الفرعية الرابعة :لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للمؤهل العلمي.

لاختبار هذه الفرضيات تم استخدام اختبار (Mann - Whitney) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للمؤهل العلمي، وقد عمل الباحث على دمج فئة دبلوم كلية مجتمع وبين فئة البكالوريوس إذ إن أفراد عينة الدراسة في دبلوم كلية مجتمع قليلون نسبياً بالإضافة للدمج بين فئات دبلوم الدراسات العليا والماجستير والدكتوراه وذلك كون أفراد هذه العينات قليلين نسبياً وكما هو موضح بالجدول رقم (4-4-8)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير المؤهل العلمي وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-8)

المتغير: المؤهل العلمي				
رقم الفقرة	الفقرة	بكالوريوس فأقل	دبلوم دراسات عليا فأكثر	P-Value
التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack)				
10	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	4.14	4.85	0.049
11	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم	4.14	4.92	0.014
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	4.08	4.85	0.047
14	اختبار النظام والتدقيق عليه بشكل دوري	3.93	4.69	0.048
هجمات حقن قواعد البيانات (SQL Injection Attack)				
22	اختبار النظام والتدقيق عليه بشكل دوري	3.97	4.54	0.041
إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin)				
26	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	3.95	4.69	0.045
28	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.97	4.85	0.007

31	وجود فريق استجابة للتهديدات التي تعرض لها النظام	4.00	4.69	0.030
32	تحديث البرمجيات المتخصصة بشكل دوري	4.08	5.00	0.000
إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft)				
40	تحديث البرمجيات المتخصصة بشكل دوري	3.92	4.69	0.041
الفيروسات (Viruses)				
58	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	4.24	4.85	0.042
62	اختبار النظام والتدقيق عليه بشكل دوري	4.22	4.92	0.011

بالإشارة للجدول رقم (4-4-8) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا بين أفراد العينة تعود إلى المؤهل العلمي، ويلاحظ من الجدول السابق بأنه 12 فقرة فقط أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة أي أن الغالبية العظمى لم ينتج عنها فروق إحصائية مهمة تعود إلى المؤهل العلمي ويلاحظ أن المتوسطات الحسابية في الجدول موزعة بشكل شبه عشوائي، وعليه **لا ترفض الفرضية العدمية** أي لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للمؤهل العلمي.

الفرضية الفرعية الخامسة: لا توجد فروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد سنوات الخبرة.

لاختبار هذه الفرضيات تم استخدام اختبار (Kruskal - Wallis test) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد سنوات الخبرة، وقد عمل الباحث على دمج فئة سنوات الخبرة (11 و 15 سنة) و (16 و 20 سنة) و(أكثر من 20 سنة) إذ إن أفراد عينة الذين يمتلكون خبرات أكثر من 15 سنة قليلين نسبياً وكما هو موضح بالجدول رقم (4–4–9)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير عدد سنوات الخبرة وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-9)

المتغير: عدد سنوات الخبرة					
رقم الفقرة	الفقرة	دون 5 سنوات	بين 5 و 10سنوات	أكثر من 10 سنوات	P-Value
اختراق الشبكة والإطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة (Password cracking)					
2	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	4.52	5.00	4.79	0.024

4	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	4.13	4.78	4.71	0.026
8	تحديث البرمجيات المتخصصة بشكل دوري	3.87	4.67	4.71	0.002
التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack)					
9	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة	3.55	4.11	4.43	0.016
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.90	4.37	4.64	0.030
16	تحديث البرمجيات المتخصصة بشكل دوري	3.84	4.37	4.71	0.002
هجمات حقن قواعد البيانات (SQL Injection Attack)					
20	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.87	4.48	4.71	0.011
22	اختبار النظام والتدقيق عليه بشكل دوري	3.68	4.33	4.43	0.049
24	تحديث البرمجيات المتخصصة بشكل دوري	3.74	4.37	4.79	0.003
إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin)					
30	اختبار النظام والتدقيق عليه بشكل دوري	3.90	4.15	4.71	0.047
32	تحديث البرمجيات المتخصصة بشكل دوري	3.84	4.41	4.86	0.007
إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft)					

34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	3.77	4.30	4.64	0.032
36	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.81	4.48	4.43	0.016
40	تحديث البرمجيات المتخصصة بشكل دوري	3.58	4.33	4.57	0.003
وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة (Phishing)					
42	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	3.90	4.22	4.71	0.020
44	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.48	4.07	4.57	0.022
48	تحديث البرمجيات المتخصصة بشكل دوري	3.55	4.41	4.64	0.000
حصان طروادة (Trojan Horse): وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال					
50	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	3.65	4.30	4.50	0.014
51	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم	3.71	4.59	4.57	0.010
52	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.71	4.59	4.71	0.010
56	تحديث البرمجيات المتخصصة بشكل دوري	3.61	4.59	4.64	0.004

الفيروسات (Viruses)					
64	تحديث البرمجيات المتخصصة بشكل دوري	4.00	4.78	4.71	0.002
البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware)					
72	تحديث البرمجيات المتخصصة بشكل دوري	3.58	4.33	4.64	0.001
المعوقات / التحديات التي تؤثر على تفعيل إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية					
73	عدم الخضوع لتدريب مستمر حول أساليب الاحتيال الإلكتروني	4.10	3.81	4.79	0.007
75	عدم التزام مستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة	3.97	3.70	4.71	0.028
77	عدم اهتمام ودعم الإدارة العليا لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات	4.13	3.89	4.79	0.011

بالإشارة للجدول رقم (4-4-9) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا بين أفراد العينة تعود إلى عدد سنوات الخبرة، ويلاحظ من الجدول السابق بأنه 26 فقرة أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة، ويلاحظ تركز الفروق في إجراءات المنع والتصحيح، إذ يلاحظ انخفاض المتوسطات الحسابية لأفراد العينة ذوي الخبرات التي أقل من 5 سنوات، وقد يعود ذلك لعدم وعي هذه الفئة بدرجة كافية لمدى فاعلية هذه الإجراءات، وعليه **ترفض**

الفرضية العدمية أي توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد سنوات الخبرة.

الفرضية الفرعية السادسة : لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للحصول على شهادات مهنية.

لاختبار هذه الفرضيات تم استخدام اختبار (Mann - Whitney) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للحصول على شهادات مهنية، كما هو موضح بالجدول رقم (4-4-10)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير الحصول على شهادات مهنية وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-10)

المتغير: الحصول على شهادات مهنية				
رقم الفقرة	الفقرة	نعم	لا	P-Value
اختراق الشبكة والإطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة (Password cracking)				
8	تحديث البرمجيات المتخصصة بشكل دوري.	4.58	4.21	0.035

التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack)				
9	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.33	3.73	0.016
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	4.67	4.00	0.025
16	تحديث البرمجيات المتخصصة بشكل دوري	4.67	3.98	0.003
إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin)				
25	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.33	3.63	0.013
28	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	4.54	3.92	0.043
29	إنشاء سجل دخول نظام المعلومات المحاسبي والشبكة الحاسوبية	4.58	3.92	0.028
32	تحديث البرمجيات المتخصصة بشكل دوري	4.67	4.04	0.027
إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft)				
33	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.46	3.73	0.012
34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.71	3.85	0.002
35	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.71	3.81	0.004

37	إنشاء سجل دخول نظام المعلومات المحاسبي والشبكة الحاسوبية	4.54	3.71	0.006
38	اختبار نظام المعلومات المحاسبي والشبكة الحاسوبية والتدقيق عليهما بشكل دوري.	4.54	3.83	0.011
39	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	4.33	3.75	0.046
وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة (Phishing)				
41	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	4.50	3.77	0.028
48	تحديث البرمجيات المتخصصة بشكل دوري	4.50	3.88	0.022
حصان طروادة : وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال				
52	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	4.71	4.00	0.010
56	تحديث البرمجيات المتخصصة بشكل دوري	4.67	3.94	0.004
الفيروسات (Viruses)				
58	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	4.67	4.19	0.012
59	تحديد صلاحيات مستخدمين النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.79	4.31	0.029
64	تحديث البرمجيات المتخصصة بشكل دوري	4.83	4.23	0.002

البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware)				
72	تحديث البرمجيات المتخصصة بشكل دوري	4.50	3.85	0.015
المعوقات / التحديات التي تؤثر على تفعيل إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية				
78	ارتفاع كلفة تنفيذ إجراءات الرقابة الداخلية على أمن المعلومات.	4.13	3.73	0.040

بالإشارة للجدول رقم (4-4-10) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا بين أفراد العينة تعود إلى الحصول على شهادات مهنية، ويلاحظ من الجدول السابق بأن 23 فقرة أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة، ويلاحظ أن المتوسطات الحسابية في الجدول في حالة وجود مؤهل مهني أكبر من حالة عدم وجود مؤهل مهني إلا أن الفقرات المذكورة مأخوذة من أكثر من مجال في الاستبانة، وأن أغلب الفروق كانت في الاستجابات المطبقة في "التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة"، وعليه **ترفض الفرضية العدمية** أي أنه توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً للحصول على شهادات مهنية.

الفرضية الفرعية السابعة : لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لتصنيف الشركة.

لاختبار هذه الفرضيات تم استخدام اختبار (Mann - Whitney) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لتصنيف الشركة، كما هو موضح بالجدول رقم (4-4-11)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير لتصنيف الشركة، وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-11)

المتغير: تصنيف الشركة				
رقم الفقرة	الفقرة	شركة محلية	شركة أجنبية	P-Value
التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack)				
9	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.54	4.34	0.005
10	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.89	4.66	0.033
11	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	3.92	4.66	0.037
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.84	4.63	0.016

14	اختبار نظام المعلومات المحاسبي والشبكة الحاسوبية والتدقيق عليهما بشكل دوري.	3.68	4.49	0.007
15	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.68	4.43	0.011
16	تحديث البرمجيات المتخصصة بشكل دوري	3.84	4.60	0.007
هجمات حقن قواعد البيانات (SQL Injection Attack)				
18	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.95	4.51	0.038
19	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.00	4.54	0.027
20	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.97	4.57	0.019
22	اختبار نظام المعلومات المحاسبي والشبكة الحاسوبية والتدقيق عليهما بشكل دوري.	3.76	4.40	0.006
23	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.81	4.49	0.006
24	تحديث البرمجيات المتخصصة بشكل دوري	3.92	4.46	0.015
إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به (Evil Twin)				

32	تحديث البرمجيات المتخصصة بشكل دوري	3.89	4.63	0.016
إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft)				
33	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.62	4.34	0.022
34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.78	4.51	0.036
35	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	3.73	4.51	0.019
36	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.84	4.54	0.005
38	اختبار نظام المعلومات المحاسبي والشبكة الحاسوبية والتدقيق عليهما بشكل دوري.	3.65	4.51	0.006
حصان طروادة (Trojan Horse): وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال				
49	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	3.62	4.34	0.046
50	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	3.78	4.34	0.037
51	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	3.86	4.57	0.034

52	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.81	4.69	0.003
55	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.81	4.46	0.033
56	تحديث البرمجيات المتخصصة بشكل دوري	3.81	4.57	0.023
الفيروسات (Viruses)				
59	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	4.22	4.74	0.035
63	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	4.08	4.57	0.041
64	تحديث البرمجيات المتخصصة بشكل دوري	4.14	4.74	0.019
البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware)				
68	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة الحاسوبية	3.73	4.40	0.034
71	وجود فريق استجابة للتهديدات التي تعرض لها نظام المعلومات المحاسبي والشبكة الحاسوبية	3.57	4.23	0.042
72	تحديث البرمجيات المتخصصة بشكل دوري	3.73	4.43	0.012

بالإشارة للجدول رقم (4-4-11) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا للعينة تعود إلى تصنيف الشركة، ويلاحظ من الجدول السابق بأن 31 فقرة أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة، إذ يلاحظ بأن استجابات العاملين في الشركات المحلية كانت متوسطة بينما استجابات العاملين في الشركات الاجنبية كانت مرتفعة، وقد يعود ذلك لاهتمام الشركات الأجنبية بإجراءات الرقابة الداخلية وذلك بسبب طبيعة البعد الجغرافي بين فروعها وبالتالي ضمان حماية أصولها المنتشرة في المناطق الجغرافية المختلفة. وعليه **ترفض الفرضية العدمية** أي أنه توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لتصنيف الشركة.

الفرضية الفرعية الثامنة: لا توجد فروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد الموظفين.

لاختبار هذه الفرضية تم استخدام اختبار (Mann - Whitney) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد الموظفين، وقد عمل الباحث على دمج فئة عدد الموظفين العاملين في الشركة بين (أقل من 50 موظف) وبين (من 50 إلى 100 موظف) إذ إن أفراد هذه العينة قليلون نسبياً وكما هو موضح بالجدول رقم (4-4-12)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير عدد الموظفين وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-12)

المتغير: عدد الموظفين في الشركة				
رقم الفقرة	الفقرة	100 موظف فأقل	أكثر من 100 موظف	P-Value
اختراق الشبكة والإطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة (Password cracking)				
1	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة	3.40	4.35	0.040
2	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	4.30	4.82	0.041
4	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.80	4.60	0.012
8	تحديث البرمجيات المتخصصة بشكل دوري	3.50	4.47	0.040
هجمات حقن قواعد البيانات (SQL Injection Attack)				
20	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.20	4.44	0.002
22	اختبار النظام والتدقيق عليه بشكل دوري	3.10	4.23	0.017
23	وجود فريق استجابة للتهديدات التي تعرض لها النظام	3.20	4.29	0.030
24	تحديث البرمجيات المتخصصة بشكل دوري	3.00	4.37	0.002

إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft)				
34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	3.30	4.27	0.014
35	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	3.10	4.27	0.020
36	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.40	4.31	0.009
وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة (Phishing)				
41	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة	3.00	4.18	0.049
48	تحديث البرمجيات المتخصصة بشكل دوري	3.20	4.23	0.036
حصان طروادة (Trojan Horse): وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال				
49	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة	2.70	4.18	0.005
51	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم	3.30	4.35	0.012
52	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	2.90	4.45	0.002

54	اختبار النظام والتدقيق عليه بشكل دوري	3.10	4.32	0.012
56	تحديث البرمجيات المتخصصة بشكل دوري	3.00	4.37	0.023
الفيروسات (Viruses)				
59	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم	3.70	4.60	0.006
60	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	3.60	4.53	0.017
61	إنشاء سجل دخول للنظام	3.50	4.39	0.021
64	تحديث البرمجيات المتخصصة بشكل دوري	3.70	4.55	0.018
البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware)				
65	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة	2.60	4.10	0.009
66	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك	3.20	4.21	0.047
68	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة	2.90	4.24	0.007
69	إنشاء سجل دخول للنظام	3.00	4.18	0.036
71	وجود فريق استجابة للتهديدات التي تعرض لها النظام	2.70	4.08	0.009
72	تحديث البرمجيات المتخصصة بشكل دوري	3.10	4.23	0.040

بالإشارة للجدول رقم (4-4-12) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا للعينة التي تعود إلى عدد الموظفين في الشركة، ويلاحظ من الجدول السابق بأنه 28 فقرة أظهرت فروق ذات أهمية إحصائية من أصل 78 فقرة، ويلاحظ بأن متوسط استجابات العاملين في الشركات التي يعمل بها "100 موظف فأقل" منخفضة بشكل ملحوظ وهي تتراوح بين منخفضة ومتوسطة، على الرغم من ارتفاع متوسط استجابات العاملين في الشركات التي يعمل بها أكثر من 100 موظف، وقد يعود ذلك لبساطة وسهولة التواصل بين المستويات الإدارية المختلفة في الشركات الصناعية التي يعمل بها 100 موظف فأقل والذي أدى لاعتقادهم بعدم ضرورة تكبد تكاليف مرتفعة نسبياً لتطبيق إجراءات رقابة داخلية قوية في شركاتهم، وعليه **ترفض الفرضية العدمية** أي أنه توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لعدد الموظفين.

الفرضية الفرعية التاسعة : لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لنوع الشركة.

لاختبار هذه الفرضيات تم استخدام اختبار (Mann - Whitney) وذلك من أجل التحقق من الفروق في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لنوع الشركة كما هو موضح بالجدول رقم (4-4-13)، ويوضح الجدول المتوسط الحسابي لكل فئة من فئات متغير نوع الشركة وذلك للفقرات التي أظهر الاختبار أنه يوجد فيها فروق ذات دلالة إحصائية مهمة عند مستوى معنوية (0.05)، وقد عمل الباحث على استثناء الفقرات التي لا ينتج عنها فروق مهمة إحصائيا إذ إن إضافتها لن يكون مفيداً للمعلومات المعروضة.

جدول رقم (4-4-13)

المتغير: نوع الشركة				
رقم الفقرة	الفقرة	مساهمة عامة	ذات مسؤولية محدودة	P-Value
معوقات تطبيق إجراءات الرقابة الداخلية				
78	ارتفاع كلفة تنفيذ إجراءات الرقابة الداخلية على أمن المعلومات.	3.42	4.11	0.027

بالإشارة للجدول رقم (4-4-13) فإن الجمل الواردة فيه هي التي وجد فيها فروق مهمة إحصائيا للعينة تعود إلى عدد الموظفين في الشركة، ويلاحظ من الجدول السابق بأنه فقط فقرة واحدة هي التي أظهرت فرق ذا أهمية إحصائية من أصل 78 فقرة أي أن الغالبية العظمى لم ينتج عنها فروق إحصائية مهمة تعود إلى نوع الشركة، ونظراً لعدم وجود سوى فرق واحد فقط **لا ترفض الفرضية العدمية** أي أنه لا توجد فروق ذات دلالة إحصائية في اجابات أفراد عينة الدراسة تعود إلى الخلفية الشخصية لكل منهم تبعاً لنوع الشركة.

والخلاصة بالنسبة للفرضية الرئيسية الخامسة أنه توجد فروق هامة احصائياً تعزى للخلفية الشخصية لأفراد عينة الدراسة في مجالات الدور الوظيفي وعدد سنوات الخبرة والحصول على شهادات مهنية وتصنيف الشركة وعدد الموظفين العاملين في الشركة ونوع الشركة، بينما لا توجد فروق مهمة احصائيا في مجالات العمر والرتبة الوظيفية والمؤهل العلمي ونوع الشركة.

ويمكن توضيح الفروق الهامة احصائياً بالشكل التالي:

1- قلة إدراك المحاسبين العاملين في الشركات الصناعية الأردنية لإجراءات الرقابة الداخلية المتبعة في هذه الشركات لحماية أصولها المعلوماتية، مقارنة مع نظرائهم العاملين في التدقيق الداخلي وتكنولوجيا المعلومات.

2- قلة وعي فئة الموظفين الذين يمتلكون سنوات خبرة أقل من خمسة سنوات بدرجة كافية لمدى فاعلية إجراءات الرقابة الداخلية على أمن المعلومات الالكترونية.

3- يمتلك الموظفون الحاصلون على شهادات مهنية درجة أعلى من الإدراك بأهمية الرقابة على أمن المعلومات الالكترونية مقارنة بالموظفين الذين لا يمتلكون مثل هذه الشهادات.

4- درجة فاعلية إجراءات الرقابة الداخلية على أمن المعلومات الالكترونية أعلى في الشركات الاجنبية منها في الشركات المحلية.

5- درجة فاعلية إجراءات الرقابة الداخلية على أمن المعلومات الالكترونية أعلى في الشركات التي يعمل فيها أكثر من 100 موظف منها في الشركات التي يعمل فيها 100 موظف فأقل.

الفصل الخامس

الاستنتاجات والتوصيات

الفصل الخامس

الاستنتاجات والتوصيات

5-1 المقدمة

5-2 الاستنتاجات

5-3 التوصيات

5-1 المقدمة:

هدفت الدراسة إلى استكشاف دور إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية، ولقد وضع الباحث عدداً من الأسئلة والفرضيات التي تتعلق بالدراسة وتوصل إلى عدة استنتاجات ساهمت في حل المشكلة والإجابة عن أسئلة الدراسة، وكما يلي:

5-2 الاستنتاجات:

أظهرت نتائج التحليل الإحصائي فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية من خلال أوجهها الثلاثة (المنع والاكتشاف والتصحيح) وكذلك فاعلية هذه الإجراءات على ثلاثة أنواع من المخاطر التي تهدد أمن المعلومات الالكترونية وهي مخاطر اختراق الشبكات والهندسة الاجتماعية والبرمجيات الضارة، أضف إلى ذلك وجود فروق ذات دلالة إحصائية بين إجابات أفراد العينة تعود للخلفية الشخصية لكل منهم.

وعلى الرغم من أن النتائج أظهرت فاعلية إجراءات الرقابة الداخلية على أمن المعلومات الالكترونية في الشركات الصناعية الأردنية إلا أن درجة هذه الفاعلية كانت تعتمد على عاملين اثنين وهما وجود مدققين داخليين يعملون ضمن كادر الشركة كون النتائج أظهرت عدم وجود الوعي الكافي لدى المحاسبين والماليين بهذه الإجراءات، وأيضاً وجود موظفين حاصلين على شهادات مهنية مما له دور في تعزيز فاعلية إجراءات الرقابة الداخلية.

كذلك أظهرت النتائج بأن درجة فاعلية إجراءات الرقابة الداخلية على أمن المعلومات الالكترونية أعلى في الشركات الاجنبية منها في الشركات المحلية، وقد يعود ذلك لعدة اسباب منها

البعد الجغرافي عن الشركة الأم الذي أدى لإلزام هذه الشركات بالعمل على معايير صارمة لضمان المحافظة على اصولها، بالإضافة لذلك أظهرت الدراسة بأن الشركات التي يعمل فيها 100 موظف فأقل لا تلتزم بتطبيق إجراءات الرقابة الداخلية على أمن معلوماتها بدرجة كافية، وقد يعود ذلك إلى انخفاض المخاطر الالكترونية التي قد تتعرض لها هذه الشركات مقارنة مع كلفة تطبيق إجراءات قوية وفعالة للرقابة على أمن معلوماتها.

أظهرت النتائج أيضاً وجود معوقات وتحديات تواجه تطبيق إجراءات رقابة داخلية فعالة ومنها عدم خضوع الموظفين لتدريب بالقدر الكافي حول اساليب الاحتيال الإلكتروني وقد يكون ذلك بسبب الكلفة المرتفعة لمثل هذا النوع من التدريب، وعدم وعي مستخدمي نظم المعلومات المحاسبية بأهمية الرقابة على أمن المعلومات، وعدم التزام مستخدمي النظام بسياسات الشركة المتعلقة بأمن المعلومات، بالإضافة للتطور المتسارع لأساليب الاحتيال الإلكتروني، وأيضا عدم دعم الإدارة لأنشطة الرقابة الداخلية المتعلقة بهذا الشأن، وأخيراً ارتفاع كلفة تنفيذ إجراءات الرقابة الداخلية على أمن المعلومات.

5-3 التوصيات:

استنادا إلى نتائج التحليل الإحصائي والاستنتاجات التي تم التوصل إليها خرجت الدراسة بالتوصيات التالية:

1- ضرورة دعم الإدارة لأنشطة الرقابة الداخلية على أمن المعلومات من خلال توفير الكوادر المؤهلة في قسم التدقيق الداخلي بالإضافة لتوفير التدريب اللازم لهم للتعرف على التحديات الجديدة التي تواجه أمن المعلومات وأساليب مكافحتها.

2- ضرورة توفير التدريب والتوعية لموظفي الإدارة المالية بأهمية الأصول المعلوماتية وأساليب المحافظة عليها وخصوصاً من المخاطر الالكترونية مع التركيز على الموظفين الأقل خبرة.

3- تشجيع الموظفين العاملين في الشركات الصناعية الأردنية للحصول على الشهادات المهنية ذات العلاقة بالرقابة على أمن المعلومات.

4- ضرورة توعية الشركات التي يعمل فيها 100 موظف فأقل بأهمية تطبيق إجراءات رقابة داخلية فعالة تتناسب مع حجم نشاطها للمحافظة على أمن معلوماتها، وذلك لأن الحفاظ على سرية المعلومات الخاصة بالشركة هو أحد العناصر المهمة لتطورها الاستراتيجي.

5- ضرورة التعاون والتنسيق المستمر بين دائرة التدقيق الداخلي ودائرة تكنولوجيا المعلومات والدائرة المالية فيما يتعلق بأمن المعلومات.

قائمة المراجع

أولا: قائمة المراجع العربية:

1- البحيصي، عصام و الشريف، حرية (2008). "مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة"، **مجلة الجامعة الإسلامية (سلسلة الدراسات الإنسانية)**، 16 (2)، ص 895-923.

2- الحسبان، عطا الله، 2008. "مدى مواكبة المدققين الداخليين لمتطلبات تكنولوجيا معلومات أنظمة الرقابة الداخلية في الشركات المساهمة العامة الأردنية"، **المنارة**، 14 (1)، ص 221-281.

3- الحفناوي، محمد يوسف (2001). **نظم المعلومات المحاسبية**، عمان: دار وائل للنشر والتوزيع.

4- الحكيم، سليم مسلم، 2010، "إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمته للمؤسسات العامة ذات الطابع الإقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية"، **مجلة جامعة دمشق للعلوم الإقتصادية والقانونية**، 26 (1)، ص 563-592.

5- حمادة، رشا، 2010، "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية (دراسة ميدانية)"، **مجلة جامعة دمشق للعلوم الإقتصادية والقانونية**، 26 (1)، ص 305-334

6- الخطيب، رائد صالح (2012)، " **مدى التزام مكاتب التدقيق في الأردن بنموذج مخاطر التدقيق: دراسة ميدانية** "، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، الأردن.

7- الرحاحلة، محمد، 2010، "فاعلية متطلبات نظام الرقابة الداخلية على تكنولوجيا المعلومات في الوزارات والمؤسسات العامة الأردنية"، **دراسات العلوم الإدارية**، 30، ص 81- 110

8- الرمحي، نضال و الذيبة، زياد (2011). **نظم المعلومات المحاسبية**، عمان: دار المسيرة للنشر.

9- القشي، ظاهر شاهر (2003). **مدى فاعلية نظم المعلومات المحاسبية في تحقيق الأمان والتوكيدية والموثوقية في ظل التجارة الالكترونية**. رسالة دكتوراه، جامعة عمان العربية، عمان، الأردن.

10- مشتهى، صبري وحمدان، علام و شكر، طلال، 2011، "مدى موثوقية نظم المعلومات المحاسبية وأثرها في تحسين مؤشرات الأداء المصرفي دراسة مقارنة على المصارف الأردنية والفلسطينية المدرجة ببورصتي عمان ونابلس"، **دراسات العلوم الإدارية**، 38 (1)، ص 21-46

ثانيا: قائمة المراجع الأجنبية:

1- Abdullatif, M & Kawuq, S,(2012)" The role of internal auditing in risk management Evidence from banks in Jordan" Paper presented at the 16th International Business Research conference, Dubai,UAE,12-13 April.

2- Bagranoff, N, Simkin, M & Norman, C, (2005), **Core Concepts of Accounting Information Systems**, 9th edition, Manhattan: John Wiley and Sons.

3- Boczko, T, (2012), **Introduction to Accounting Information Systems**, England: Pearson Education.

4- Boockholdt, J, (1999), **Accounting Information Systems**, 5th edition, Singapore: McGraw-Hill

5- Committee of Sponsoring Organizations of the Treadeway Commission (1994**) Internal Control – Integrated Framework**.

6- Elder, R , Beasley, M & Arens, A, (2010), **Auditing and Assurance Services,** 13th edition, USA: Pearson Education.

7- Fulford, H & Doherty, N, (2003) "The application of information security policies in large UK-based organizations: an exploratory investigation", **Information Management and Computer Security**,11 (3), pp 106 - 114

8- Gupta, A & Hammond, R, (2005) "Information systems security issues and decisions for small businesses: An empirical examination" **Information Management and Computer Security**, 13 (4), pp 297 – 310

9- Hall, J, Sarkani, S & Mazzuchi, T, (2011) "Impacts of organizational capabilities in information security" **Information Management and Computer Security**, 19 (3), pp 155 - 176

10- Hayale, T & Abu Khadra, H, (2006) "Evaluation of the effectiveness of control systems in computerized accounting information systems: An empirical research applied on Jordanian banking sector" **Journal of Accounting, Business and Management**, 13, pp 39-68.

11- Hayes, R , Dassen, R , Schilder, A & Wallage, P, (2005), **Principles of Auditing: An Introduction to International Standards on Auditing**, 2nd edition, England: Pearson Education.

12- Joo, J, Kim, M, Normatov, I & Kim, L. (2011) "Determinants of information security affecting adoption of web-based integrated information systems" **World Academy of Science, Engineering and Technology**, 78, pp 371-376.

13- Lind, D, Marchal, W & Wathen, S, (2010), **Statistical Techniques in Business and Economics**, 14th edition, The McGraw-Hill Companies Inc.

14- Norman, A & Yasin, N, (2010), "An analysis of information system security management (ISSM): The hierarchical organizations vs emergent organization" **International Journal of Digital Society**, 1 (3), pp 230-237.

15- Porter, B , Simon, J & Hatherly, D, (2008), **Principles of External Auditing**, 3rd edition, England: John Wiley and Sons.

16- Raval, V & Fichadia, A, (2007), **Risk, Controls, and Security: Concepts and Applications**, England: John Wiley and Sons.

17- Romney, M. & Steinbart, P, (2012), **Accounting Information Systems**", 12th edition, England: Pearson Education.

18- Saunders, M , Lewis, P & Thornhill, A. (2012) **Research Methods for Business Students** 6th edition, England: Pearson Education..

19- Smith, R. (2009) "Information security – A critical business function" **Journal of GXP Compliance**, 13 (4), pp 62-68.

20- Soltani,B, (2007), **Auditing: An International Approach**, England: Pearson Education.

الملحق (1)

بسم الله الرحمن الرحيم

جامعة الشرق الأوسط

كلية الأعمال

قسم المحاسبة والتمويل

السيد/السيدة المستجيب المحترم/المحترمة

تحية طيبة،

الاستبيانة المرفقة هي جزء من بحث يقوم به الباحث **يوسف خليل عبدالجابر** استكمالا لمتطلبات الحصول على درجة الماجستير في المحاسبة من جامعة الشرق الأوسط. يتناول البحث **مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية**.

لقد تم اختيارك ضمن مجموعة من المحاسبين والمدققين الداخليين والموظفين في قسم تكنولوجيا المعلومات الذين يتميزون بدرجة عالية من التأهيل العلمي والمهني للمشاركة في هذه الاستبانة، و يرجو الباحث أن تتكرم بمنحه بعضا من وقتك الثمين للمشاركة بتعبئة هذه الاستبانة مؤكدا لكم بأن جميع البيانات التي ستدلون بها سوف تستعمل لغايات الدراسة والبحث العلمي فقط وأنها سوف تعامل بسرية تامة. وفي حالة نشر البحث أو تقديمه في مؤتمر علمي ستكون النتائج المذكورة مجمعة ولا تتعلق بشخص محدد أو شركة بعينها.

هذه الاستبانة تطرح مجموعة من الأسئلة المتعلقة بالخبرة المهنية للمستجيب ثم مجموعة من الأسئلة التي تهدف لمعرفة مدى فاعلية إجراءات الرقابة الداخلية الشائعة في مواجهة التهديدات المرتبطة باستخدام نظم المعلومات المحاسبية الإلكترونية.

في حال رغبت في الاستفسار عن أي شيء ورد في الاستبانة رجاء لا تتردد في الاتصال بالباحث على الرقم التالي(079XXXXXXX)

وشكرا لكم حسن تعاونكم.

الباحث

يوسف عبدالجابر

أولا :- <u>البيانات الشخصية</u>:-

*** أرجو منكم التكرم بوضع إشارة (×) عند الاختيار المناسب:-**

1) العمر :-

أ- أقل من 25 سنة □ ب- بين 25 و 30 سنة □ ج- بين 31 و 40 سنة □

د- بين 41 و 50 سنة □ هـ- أكثر من 50 سنة □

2) الدور الوظيفي الحالي في الشركة:-

أ- المحاسبة والإدارة المالية Accounting & Financial Management □ ب- التدقيق والرقابة داخلية Internal Audit & Control □ ج- تكنولوجيا المعلومات وأنظمة المعلومات الحاسوبية CIS & IT □

د- أخرى الرجاء ذكرها ----------

3) الرتبة الوظيفية:-

أ- موظف مبتدئ Junior □ ب- موظف رئيسي Senior □ ج- مسؤول قسم Chief □

د- مدير دائرة Manager □ هـ- غير ذلك ----------

4) المؤهل العلمي:-

أ- دبلوم كلية مجتمع فأقل □ ب- بكالوريوس □ ج- دبلوم دراسات عليا □

د- ماجستير □ ه- دكتوراه □

5) عدد سنوات الخبرة في مجال عملك:

أ- دون 5 سنوات □ ب- بين 5 و 10 سنوات □ ج- بين 11 و 15 سنة □

د- بين 16 و 20 سنة □ ه- أكثر من 20 سنة □

6) الحصول على الشهادات المهنية (مثلا CPA, CMA, CIA, SISCO):

أ- نعم □ ب- لا □

ثانيا :- <u>معلومات خاصة بالشركة</u>:

1) تصنف الشركة على أنها:
أ- شركة محلية □ ب- شركة أجنبية □

2) عدد الموظفين في الشركة التي تعمل لديها حاليا:

أ- دون 50 موظف □ ب- من 50 إلى 100 موظف □ ج- أكثر من 100 □

3) نوع الشركة:

أ- مساهمة عامة □ ب- مساهمة خاصة □ ج- غير ذلك _____

ثالثا:- تعتبر العوامل التالية من أبرز المشاكل التي تتعرض لها أنظمة المعلومات المحاسبية في الشركات الصناعية. لكل من العوامل (التهديدات) التالية والتي قد تتعرض لها شركتكم يرجى الإشارة بوضع علامة (X) والتي توضح **مدى فاعلية الإجراءات الرقابية المذكورة أدناه في شركتكم** للحد من أثر العامل المشار إليه.

(الباحث إذ يقدر وقتكم الثمين فإنه لا يتوقع بأن يستغرق تعبئة الإستبانة وقتاً طويلاً جداً وذلك لأن الأسئلة المرفقة متشابهة تماماً لجميع العوامل)

- العامل الأول: اختراق الشبكة والإطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة (Password cracking):

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
1	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
2	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
3	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
4	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
5	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
6	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
7	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
8	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

- العامل الثاني: التعرض للاختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack):

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
9	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
10	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
11	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
13	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
14	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
15	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
16	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

- العامل الثالث: هجمات حقن قواعد البيانات (SQL Injection Attack):
مثلا من خلال إدخال برمجية ضارة مكان كلمة السر أو إسم المستخدم بحيث تمكن المحتال من الوصول إلى قواعد البيانات بهدف سرقتها أو التعديل فيها أو تدميرها.

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
17	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
18	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
19	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
20	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
21	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
22	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
23	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
24	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

- العامل الرابع: إدعاء جهة معينة بأنها جهة موثوق بها من قبل المستخدم تطلب منه إستخدام ملف مرفق يكون ضارا به (Evil Twin):

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
25	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
26	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
27	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
28	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
29	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
30	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
31	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
32	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

- العامل الخامس: إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم ، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر (Identity theft):

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
33	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
34	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
35	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
36	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
37	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
38	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
39	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
40	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

العامل السادس: وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة (Phishing):

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
41	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
42	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
43	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
44	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
45	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
46	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
47	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
48	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

- العامل السابع: حصان طروادة (Trojan Horse):

وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال.

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
49	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
50	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
51	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
52	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
53	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
54	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
55	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
56	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

- العامل الثامن: الفيروسات (Viruses):
وهي برنامج يدخل إلى الحاسوب ويتصل بالملفات المخزنة به ثم يكرر نفسه بحيث يتم تدمير هذه الملفات.

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
57	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
58	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
59	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
60	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
61	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
62	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
63	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
64	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

- العامل التاسع: البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت (Spyware):

الرقم	إجراءات الرقابة	غير متوفرة	غير فعالة بشكل كبير	غير فعالة بشكل قليل	فعالة بشكل قليل	فعالة بشكل كبير
65	التوعية والتدريب المستمر لمستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
66	تقييد الدخول على النظام والشبكة بالأشخاص المصرح لهم بذلك.	1	2	3	4	5
67	تحديد صلاحيات مستخدمي النظام بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.	1	2	3	4	5
68	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول على الشبكة (مثلا: مقاوم الفيروسات (Anti Virus)، والجدار الناري (Firewall))	1	2	3	4	5
69	إنشاء سجل دخول للنظام (Log File).	1	2	3	4	5
70	اختبار النظام والتدقيق عليه بشكل دوري.	1	2	3	4	5
71	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	1	2	3	4	5
72	تحديث البرمجيات المتخصصة بشكل دوري (مثلا: تحديث مقاوم فيروسات (Anti Virus) بشكل مستمر).	1	2	3	4	5

رابعا:- قد تواجه الشركات العديد من المعوقات / التحديات التي تؤثر على تفعيل إجراءات الرقابة الداخلية المرتبطة بمخاطر أمن معلومات نظم المعلومات المحاسبية الإلكترونية ، لكل من المعوقات التالية والتي قد تتعرض لها شركتكم يرجى الإشارة بوضع علامة (X) والتي توضح مدى أثر هذا المعوق على إجراءات الرقابة الداخلية.

الرقم	المعوقات	غير مؤثر	غير مؤثر بشكل كبير	غير مؤثر بشكل قليل	مؤثر بشكل قليل	مؤثر بشكل كبير
73	عدم الخضوع لتدريب مستمر حول أساليب الاحتيال الإلكتروني.	1	2	3	4	5
74	عدم وعي مستخدمي النظام بأهمية الرقابة على تكنولوجيا المعلومات	1	2	3	4	5
75	عدم التزام مستخدمي النظام بالسياسات المتعلقة بأمن المعلومات المتبعة داخل الشركة.	1	2	3	4	5
76	التطور المتسارع لأساليب الاحتيال الإلكتروني.	1	2	3	4	5
77	عدم اهتمام ودعم الإدارة العليا لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات.	1	2	3	4	5
78	ارتفاع كلفة تنفيذ إجراءات الرقابة الداخلية على أمن المعلومات.	1	2	3	4	5